Teoría de Galois
EN ELABORACIÓN

Pedro Sancho de Salas

15-06-2011

Índice general

Capítulo 1

Operaciones fundamentales del Álgebra

1.1. Espectro primo de un anillo

1. Definición : Sea A un anillo. Llamaremos espectro primo del anillo A, que denotaremos $\operatorname{Spec} A$, al conjunto de los ideales primos de A.

Recordemos que todo anillo, salvo el anillo $A = \{0\}$, contiene ideales primos. Por tanto, $\operatorname{Spec} A = \emptyset$ si y sólo si $A = \{0\}$.

2. Ejemplo : Si k es un cuerpo $\operatorname{Spec} k = \{(0)\}$ es un conjunto de orden 1.

3. Ejemplo : $\operatorname{Spec} \mathbb{Z} = \{(0), (2), (3), (5), (7), \cdots\}$. Los ideales (p), $p > 0$ primo, son ideales maximales.

4. Ejemplo : $\operatorname{Spec} \mathbb{Q}[x] = \{(0), (p(x))$, con $p(x)$ polinomio irreducible (mónico) de $\mathbb{Q}[x]\}$.
$\operatorname{Spec} \mathbb{C}[x] = \{(0), (x - \alpha)$, con $\alpha \in \mathbb{C}\}$.

Dado un morfismo de anillos $f\colon A \to B$ y un ideal primo $\mathfrak{p} \subset B$, el lector puede comprobar que $f^{-1}(\mathfrak{p}) \subset A$ es un ideal primo de A. Por tanto, tenemos una aplicación $f^*\colon \operatorname{Spec} B \to \operatorname{Spec} A$, $\mathfrak{p} \mapsto f^{-1}(\mathfrak{p})$.

5. Notación : Un ideal primo lo denotaremos con una letra (x, y,...) cuando lo consideremos como elemento de $\operatorname{Spec} A$. Cuando $x \in \operatorname{Spec} A$ lo consideremos como ideal de A lo denotaremos $\mathfrak{p}_x$.

6. Notación : Dado un ideal $I \subseteq A$ denotaremos $(I)_0 := \{x \in \operatorname{Spec} A\colon\ I \subseteq \mathfrak{p}_x\}$.

7. Proposición : *Sea $I \subseteq A$ un ideal y $\pi\colon A \to A/I$ el morfismo de paso al cociente. Entonces, se cumple la igualdad*

$$(I)_0 = \operatorname{Spec}(A/I),\ x \mapsto \pi^*(x)$$

Demostración. Tenemos la biyección de conjuntos

$$\begin{array}{rcl} [\text{Conjunto de ideales de } A \text{ que contienen a } I] & = & [\text{Conjunto de ideales de } A/I] \\ J & \longmapsto & \pi(J) = \bar{J} \\ \pi^{-1}(J') & \longleftarrow & J' \end{array}$$

Sabemos que si $\mathfrak{p}'$ es un ideal primo de A/I, entonces $\pi^{-1}(\mathfrak{p})$ es un ideal primo de A. Además, si $\mathfrak{p}$ es un ideal primo de A que contiene a I, entonces $\pi(\mathfrak{p}) = \bar{\mathfrak{p}}$ es un ideal primo de A/I: Si $\bar{a} \cdot \bar{a}' = \overline{aa'} \in \bar{\mathfrak{p}}$, entonces $aa' \in \mathfrak{p} + I = \mathfrak{p}$, luego $a \in \mathfrak{p}$ ó $a' \in \mathfrak{p}$, es decir, $\bar{a} = \bar{\mathfrak{p}}$ ó $\overline{a'} \in \bar{\mathfrak{p}}$. Por tanto,

$$\begin{array}{rcl} (I)_0 = [\text{Conj. de id. primos de } A \text{ que contienen a } I] & = & [\text{Conj. de id. primos de } A/I] = \operatorname{Spec}(A/I) \\ J & \longmapsto & \pi(J) = \bar{J} \\ \pi^{-1}(J') & \longleftarrow & J' \end{array}$$

□

8. Proposición: *Se cumple que*

1. $(I_1 \cdot I_2)_0 = (I_1 \cap I_2)_0 = (I_1)_0 \cup (I_2)_0$
2. $(I_1 + I_2)_0 = (I_1)_0 \cap (I_2)_0$.

Demostración. 1. Es obvio que $(I_1)_0 \cup (I_2)_0 \subseteq (I_1 \cap I_2)_0$. Veamos que $(I_1 \cap I_2)_0 \subseteq (I_1)_0 \cup (I_2)_0$: Si $x \in (I_1 \cap I_2)_0$ y $x \notin [(I_1)_0 \cup (I_2)_0]$, entonces existen $f_1 \in I_1$ y $f_2 \in I_2$ tales que $f_1, f_2 \notin \mathfrak{p}_x$. Por tanto, $f_1 \cdot f_2 \notin \mathfrak{p}_x$. Pero como $f_1 \cdot f_2 \in I_1 \cap I_2$, tendremos que $(I_1 \cap I_2) \underset{\neq}{\subseteq} \mathfrak{p}_x$, es decir, $x \notin (I_1 \cap I_2)_0$ y hemos llegado a contradicción. En conclusión, $(I_1 \cap I_2)_0 = (I_1)_0 \cup (I_2)_0$

Para probar que $(I_1 \cdot I_2)_0 = (I_1)_0 \cup (I_2)_0$, se argumenta igual.

2. Es obvio. □

9. Proposición: *Se cumple que*

$$\operatorname{Spec}(A \times B) = \operatorname{Spec} A \coprod \operatorname{Spec} B$$

Demostración. Sea $I_1 := ((1,0)) = A \times 0$ e $I_2 := ((0,1)) = 0 \times B$. Se tiene que $I_1 \cdot I_2 = 0$ y $I_1 + I_2 = A \times B$. Por tanto,

$$(I_1)_0 \cup (I_2)_0 = (I_1 \cdot I_2)_0 = (0)_0 = \operatorname{Spec}(A \times B)$$
$$(I_1)_0 \cap (I_2)_0 = (I_1 + I_2)_0 = (A \times B)_0 = \emptyset$$

Por lo tanto, $\operatorname{Spec}(A \times B) = (I_1)_0 \coprod (I_2)_0$. Por último, $(I_1)_0 = \operatorname{Spec}(A \times B/I_1) = \operatorname{Spec}(A \times B/A \times 0) = \operatorname{Spec} B$. Igualmente, $(I_2)_0 = \operatorname{Spec} A$.

□

10. Observación: Explícitamente, $\operatorname{Spec}(A \times B) = \{\mathfrak{p} \times B, A \times \mathfrak{q}$, para todo $\mathfrak{p} \subset A$ y $\mathfrak{q} \subset B$ ideales primos$\}$.

11. Ejercicio: Sea k un cuerpo. Calcular $\operatorname{Spec}(k \times \overset{n}{\cdots} \times k)$.

1.2. Localización de anillos

1. Definición: Sea A y $S \subseteq A$ un subconjunto. Diremos que S es un sistema multiplicativo de A si cumple

1. $1 \in S$.
2. Si $s, s' \in S$ entonces $s \cdot s' \in S$.

2. Ejemplo: $\mathbb{Z} - \{0\}$ es un sistema multiplicativo de $\mathbb{Z}$.

3. Definición: Sea A un anillo y $S \subset A$ un sistema multiplicativo de A. La localización de A por S, A_S, es el conjunto

$$A_S := \left\{ \frac{a}{s},\ a \in A \text{ y } s \in S : \frac{a}{s} = \frac{a'}{s'} \text{ si existen } s_1, s_2 \in S \text{ tales que las fracciones } \frac{s_1 a}{s_1 s}, \frac{s_2 a'}{s_2 s'} \text{ tienen el mismo numerador y denominador} \right\}^{1}$$

[1] Observemos que $\frac{a}{s} = \frac{a}{s}$, que si $\frac{a}{s} = \frac{a'}{s'}$ entonces $\frac{a'}{s'} = \frac{a}{s}$, y que si $\frac{a}{s} = \frac{a'}{s'}$ y $\frac{a'}{s'} = \frac{a''}{s''}$ entonces $\frac{a}{s} = \frac{a''}{s''}$.

Con la suma y producto ordinarios de fracciones

$$\frac{a}{s} + \frac{a'}{s'} := \frac{s'a + sa'}{ss'}$$
$$\frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}$$

A_S es un anillo. El elemento unidad de A_S es la fracción $\frac{1}{1}$. Si $s \in S$ entonces la fracción $\frac{s}{1}$ es invertible, de inverso $\frac{1}{s}$. La fracción $\frac{0}{s} = \frac{0 \cdot s}{1 \cdot s} = \frac{0}{1}$ es el elemento nulo de A_S.

4. Ejercicio: Probar que una fracción $\frac{a}{s} = 0 \in A_S$ si y sólo si existe $s' \in S$ tal que $s' \cdot a = 0$ (en A).

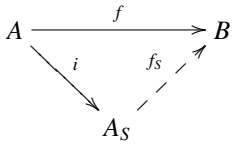
Si A es un anillo íntegro, obviamente $A_{A-\{0\}}$ es un cuerpo.

5. Ejemplo: Ejemplos de localización son los cuerpos $\mathbb{Q} = \mathbb{Z}_{\mathbb{Z}-\{0\}}$, $\mathbb{Q}(x) := \mathbb{Q}[x]_{\mathbb{Q}[x]-\{0\}}$ y más generalmente $k(x) := k[x]_{k[x]-\{0\}} = \{p(x)/q(x),\, p(x), q(x) \in k[x], q(x) \neq 0\}$, o el cuerpo de funciones racionales en n-variables con coeficientes en k,

$$k(x_1, \ldots, x_n) := k[x_1, \ldots, x_n]_{k[x_1,\ldots,x_n]-\{0\}} = \{p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n), \\ p(x_1, \ldots, x_n), 0 \neq q(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]\}$$

6. Definición: Al morfismo natural de anillos $A \to A_S$, $a \mapsto \frac{a}{1}$ se le denomina morfismo de localización por S.

7. Propiedad universal de la localización: *Sea $i\colon A \to A_S$ el morfismo de localización. Si $f\colon A \to B$ es morfismo de anillos tal que $f(s)$ es invertible para todo $s \in S$, entonces existe un único morfismo de anillos $f_S : A_S \to B$ tal que $f = f_S \circ i$, es decir, tal que el diagrama siguiente es conmutativo*



8. Ejercicio: Probar que el núcleo del morfismo de localización $A \to A_S$, es igual al ideal de elementos de A anulados por algún S.

9. Ejercicio: Probar que $(\mathbb{Z}[x])_{\mathbb{Z}-\{0\}} = \mathbb{Q}[x]$.

10. Proposición: *Sea A un anillo y $S \subseteq A$ un sistema multiplicativo. Entonces, $A_S = \{0\} \iff 0 \in S$.*

Demostración. Si $0 \in S$, entonces $\frac{a}{s} = \frac{0 \cdot a}{0 \cdot s} = \frac{0}{0}$, para todo $a \in A$ y $s \in S$. Luego, $A_S = \{0\}$, pues sólo tiene un único elemento.

Si $A_S = \{0\}$, entonces $\frac{1}{1} = \frac{0}{1}$, luego existe $s \in S$ tal que $s \cdot 1 = s \cdot 0$, luego $0 = s \in S$.

□

11. Definición: Sea A un anillo. Diremos que $a \in A$ es nilpotente si existe un número natural $n > 0$, tal que $a^n = 0$. Llamaremos radical de un anillo A, que denotaremos $\operatorname{rad} A$, al conjunto de todos los elementos de A que son nilpotentes.

12. Ejercicio: Calcular $\operatorname{rad} \mathbb{Q}[x]/(x^3)$.

13. Ejercicio: Probar que $\operatorname{rad} A$ es un ideal.

14. Proposición: *El radical de un anillo es igual a la intersección de todos los ideales primos del anillo, es decir,*

$$\operatorname{rad} A = \bigcap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$$

Demostración. Si $a \in \operatorname{rad} A$, entonces existe $n > 0$ tal que $a^n = 0$. Dado un ideal primo $\mathfrak{p}_x$, tenemos que $a^n = 0 \in \mathfrak{p}_x$, luego $a \in \mathfrak{p}_x$. Por tanto, $\operatorname{rad} A \subseteq \cap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$.

Dado $a \in \cap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$, consideremos el sistema multiplicativo $S = \{1, a, a^2, \cdots, a^n, \cdots\}$. Si $A_S \neq 0$, existe un ideal primo $\mathfrak{p} \subseteq A_S$. Sea $i \colon A \to A_S$ el morfismo de localización y el ideal primo $\mathfrak{q} = i^{-1}(\mathfrak{p}) \subset A$. Como $a \in \mathfrak{q}$, entonces $i(a) = \frac{a}{1} \in \mathfrak{p}$. Pero como $\frac{a}{1}$ es invertible tendremos que $\mathfrak{p} = (1)$ y hemos llegado a contradicción. Por tanto, $A_S = \{0\}$, luego $0 \in S$ y existe n tal que $a^n = 0$. En conclusión, a es nilpotente y $\cap_{x \in \operatorname{Spec} A} \mathfrak{p}_x \subseteq \operatorname{rad} A$. □

15. Definición : Se dice que un anillo A es reducido si $\operatorname{rad} A = 0$.

16. Ejercicio : Sea A un anillo. Probar que $A/\operatorname{rad} A$ es un anillo reducido.

1.2.1. Teorema de Gauss

17. Definición : Diremos que un elemento de un anillo íntegro es irreducible si no es nulo ni es producto de dos elementos no invertibles del anillo.

18. Definición : Un anillo íntegro se dice que es un dominio de factorización única si todo elemento del anillo es producto de elementos irreducibles, de modo único salvo orden y factores invertibles.

DFU significará dominio de factorización única.

19. Proposición : *Si A es DFU y $a \in A$ es irreducible, entonces $(a) \subset A$ es un ideal primo.*

Demostración. Sea $b \cdot c = a \cdot d$. Si consideramos las descomposición en factores irreducibles de b, c y d, y recordamos que A es DFU, tenemos que a aparece (salvo multiplicación por un invertible) en la descomposición en producto de factores irreducibles de b o c. Luego, a divide a b o c. En conclusión, $(a) \subset A$ es un ideal primo. □

20. Definición : Un polinomio $P(x) \in A[x]$ se dice *primitivo* cuando sus coeficientes no admiten un divisor común no invertible, es decir, si $P(x) = a \cdot Q(x)$ con $a \in A$, entonces a es invertible.

21. Lema : *Sea A un dominio de factorización única con cuerpo de fracciones Σ. Sean $P(x), Q(x) \in A[x]$ dos polinomios primitivos. Entonces,*

1. *$P(x) \cdot Q(x)$ es primitivo.*
2. *Si existen $a, b \in A$ tales que $a \cdot P(x) = b \cdot Q(x)$, entonces $b = a \cdot u$, para cierto invertible $u \in A$. Por tanto, si $P(x) = \frac{b}{a} \cdot Q(x)$ en $\Sigma[x]$, entonces $\frac{b}{a} = u \in A$ es un invertible de A.*

Demostración. 1. Supongamos que $P(x) \cdot Q(x) = a \cdot R(x)$, con $R(x) \in A[x]$ y $a \in A$ no invertible. Sea $p \in A$ irreducible que divida a a. Haciendo cociente en $A[X]$ por $p \cdot A[x]$, tenemos que

$$\overline{P(x)} \cdot \overline{Q(x)} = 0 \in (A/pA)[x]$$

lo cual es contradictorio, porque $(A/pA)[x]$ es íntegro y $\overline{P(x)}$ y $\overline{Q(x)}$ son no nulos.

2. Sea p un elemento irreducible que divida a a. Haciendo cociente en $A[X]$ por $p \cdot A[x]$, tenemos que $0 = \bar{b} \cdot \overline{Q(x)}$, luego $\bar{b} = 0$ y p divide a b. Dividiendo a a y b a la vez por p y repitiendo sucesivamente este proceso obtendremos que a divide a b, y por simetría que b divide a a. Luego, $b = a \cdot u$, para cierto invertible $u \in A$. □

22. Teorema: *Sea A un dominio de factorización única con cuerpo de fracciones Σ. Un polinomio no constante primitivo, $P(x) \in A[x]$, es irreducible $A[x]$ si y sólo si es irreducible en $\Sigma[x]$.*

Demostración. Supongamos que $P(x)$ es irreducible en $\Sigma[x]$. Si $P(x) = P_1(x) \cdot P_2(x)$, con $P_1(x), P_2(x) \in A[x]$, entonces como $P(x)$ es irreducible en $\Sigma[x]$, uno de los dos polinomios $P_1(x)$ o $P_2(x)$ ha de ser de grado cero, digamos $P_1(x) = a$. Como $P(x)$ es primitivo $P_1(x) = a \in A$ es invertible. En conclusión, $P(x)$, es irreducible en $A[x]$.

Supongamos que $P(x)$ es irreducible en $A[X]$. Supongamos que $P(x) = \tilde{P}_1(x) \cdot \tilde{P}_2(x)$, siendo $\tilde{P}_1(x), \tilde{P}_2(x) \in \Sigma[x]$. Eliminando denominadores podemos suponer que

$$P(x) = \frac{a}{b} P_1(x) \cdot P_2(x)$$

con $P_1(x), P_2(x) \in A[x]$, primitivos. Por el lema 1.2.21, $\frac{a}{b} = u \in A$, luego $P(x)$ no es irreducible en $A[x]$ y hemos llegado a contradicción.

□

23. Teorema (Gauss): *Si A es un dominio de factorización única, entonces $A[x]$ también lo es.*

Demostración. Sea $\Sigma = A_{A-\{0\}}$ el cuerpo de fracciones. Sea $P(x) \in A[x]$ y escribamos $P(x) = a \cdot Q(x)$, con $a \in A$ y $Q(x) \in A[x]$ primitivo. Sea

$$Q(x) = \frac{b}{c} \widetilde{Q}_1(x)^{n_1} \cdots \widetilde{Q}_r(x)^{n_r}$$

la descomposición en $\Sigma[x]$. Eliminando denominadores es claro que se puede escribir:

$$Q(x) = \frac{d}{e} \cdot Q_1(x)^{n_1} \cdots Q_r(x)^{n_r} \qquad (*)$$

con $Q_i(x) = \frac{a_i}{b_i} \widetilde{Q}_i \in A[x]$ primitivos.

- Por el lema 1.2.21, $\frac{d}{e} = u \in A$ es un invertible de A.
- Cada $Q_i(x)$ es irreducible en $A[x]$ por que lo es en $\Sigma[x]$ y por el teorema 1.2.22.

Descomponiendo $a = u' \cdot p_1^{m_1} \cdots p_s^{m_s}$ en A se obtiene una descomposición de

$$P(x) = (u' \cdot u) p_1^{m_1} \cdots p_s^{m_s} Q_1(x)^{n_1} \cdots Q_r(x)^{n_r}$$

en $A[x]$.

Unicidad: Si $P(x) = v q_1^{d_1} \cdots q_l^{d_l} P_1(x)^{s_1} \cdots P_t(x)^{s_t}$, entonces cada $P_i(x)$ es irreducible en $\Sigma[x]$ por el teorema 1.2.22. Por tanto, los polinomios $P_i(x)$ (una vez reordenados) difieren de los $Q_i(x)$ en invertibles de A y los exponentes son los mismos. Tachando los términos polinómicos comunes se obtiene salvo unidades la igualdad $q_1^{d_1} \cdots q_l^{d_l} = p_1^{m_1} \cdots p_s^{m_s}$, de donde salvo permutación de los factores es $q_i = p_i$ (salvo invertibles de A) y los exponentes iguales.

□

24. Teorema: *Los anillos $\mathbb{Z}[x_1, \ldots, x_n]$ y $k[x_1, \ldots, x_n]$ (k un cuerpo) son dominios de factorización única.*

Como corolario de la demostración anterior, se obtiene el siguiente teorema.

1.3. Producto tensorial de módulos

Sean M y N dos A-módulos. Consideremos el A-módulo libre $A^{(M \times N)}$. Sea $\{1_i\}_{i \in M \times N}$ la base estándar de $A^{(M \times N)}$, es decir, $1_i = (a_{(m,n)})_{(m,n) \in M \times N}$ es el elemento de $A^{(M \times N)}$ definido por $a_{(m,n)} = 0$ si $(m,n) \neq i$ y $a_{(m,n)} = 1$ si $(m,n) = i$. Redenotemos $(m,n) := 1_{(m,n)}$.

Sea R el submódulo de $A^{(M\times N)}$ generado por los elementos de la forma

$$\begin{array}{l}(m+m',n)-(m,n)-(m',n)\\(m,n+n')-(m,n)-(m,n')\\(am,n)-a(m,n)\\(m,an)-a(m,n)\end{array}\qquad(*)$$

para todo $m, m' \in M$, $n \in N$ y $a \in A$.

1. Definición : Llamaremos producto tensorial de M y N sobre el anillo A, al A-módulo cociente $A^{(M\times N)}/R$ y lo denotaremos $M \otimes_A N$. Cada clase $\overline{(m,n)} \in A^{(M\times N)}/R = M \otimes_A N$ la denotaremos $m \otimes n$.

De acuerdo con la definición de R tenemos que

$$\boxed{\begin{array}{l}(m+m')\otimes n = m\otimes n + m'\otimes n\\ m\otimes(n+n') = m\otimes n + m\otimes n'\\ am\otimes n = a(m\otimes n)\\ m\otimes an = a(m\otimes n)\end{array}}$$

propiedades que se expresan diciendo "el producto tensorial es A-bilineal". En realidad, el formalismo seguido, ha sido para llegar a definir "el producto" ($\otimes$) de elementos de M por N, con estas propiedades y sin más relaciones que las generadas por las relaciones de M y N y estas propiedades.

Dado que los elementos $\{(m,n)\}_{(m,n)\in M\times N}$ forman una base de $A^{(M\times N)}$ entonces los elementos $\{m\otimes n\}_{(m,n)\in M\times N}$ forman un sistema generador de $M \otimes_A N$. Por las propiedades de bilinealidad recién escritas,

$$\boxed{\text{Si } M = \langle m_i\rangle_{i\in I} \text{ y } N = \langle n_j\rangle_{j\in J}, \text{ entonces } M = \langle m_i\otimes n_j\rangle_{(i,j)\in I\times J}.}$$

2. Definición : Sea P un A-módulo. Diremos que una aplicación $f\colon M\times N \to P$ es A-bilineal si

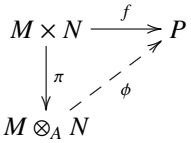
$$\begin{array}{l}f(m+m',n) = f(m,n)+f(m',n)\\ f(m,n+n') = f(m,n)+f(m,n')\\ f(am,n) = af(m,n)\\ f(m,an) = af(m,n)\end{array}$$

El conjunto de las aplicaciones A-bilineales de $M\times N$ en P se denota $\mathrm{Bil}_A(M,N;P)$. La condición de que una aplicación $f\colon M\times N\to P$ sea A-bilineal expresa que la aplicación $f_m\colon N\to P$, $f_m(n) = f(m,n)$, es un morfismo de A-módulos para cada elemento $m\in M$. Obtenemos así, un isomorfismo natural

$$\mathrm{Bil}_A(M,N;P) = \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P))$$

El morfismo natural $\pi\colon M\times N\to M\otimes N$, $(m,n)\mapsto m\otimes n$, es bilineal.

3. Propiedad universal del producto tensorial: *La aplicación $f\colon M\times N\to P$ es una aplicación bilineal si y sólo si existe un único morfismo de A-módulos $\phi\colon M\otimes_A N\to P$, de modo que el siguiente diagrama*



es conmutativo. Con concisión,

$$\mathrm{Hom}_A(M\otimes_A N, P) = \mathrm{Bil}_A(M,N;P),\quad \phi\mapsto \phi\circ\pi$$

Demostración. Sea $f\colon M \times N \to P$ una aplicación A-bilineal, entonces el morfismo de A-módulos

$$\varphi\colon A^{(M\times N)} \to P,\ \varphi(\sum_i a_i(m_i, n_i)) = \sum_i a_i f(m_i, n_i)$$

se anula sobre los generadores del submódulo R, anteriormente definido en $(*)$. Por lo tanto, induce el morfismo de A-módulos $\phi\colon M \otimes_A N \to P$, $m \otimes n \mapsto f(m, n)$. Este morfismo cumple que $f = \phi \circ \pi$ y si un morfismo ϕ' cumple esta igualdad entonces $\phi'(m \otimes n) = f(m, n)$ y coincide con ϕ, pues los elementos $m \otimes n$ generan $M \otimes N$.

Por último, es una simple comprobación ver que dado un morfismo de A-módulos $\phi\colon M \otimes N \to P$ entonces $f = \phi \circ \pi$ es una aplicación bilineal de $M \times N$ en P.

□

Así pues, este teorema nos dice que definir un morfismo de A-módulos $\phi\colon M \otimes_A N \to P$, es asignar a cada $m \otimes n \in M \otimes_A N$ un elemento $\phi(m \otimes n) \in P$ de modo que $\phi((am + m') \otimes n) = a\phi(m \otimes n) + \phi(m' \otimes n)$ y $\phi(m \otimes (an + n')) = a\phi(m \otimes n) + \phi(m \otimes n')$.

4. Observación : Análoga construcción puede hacerse para cualquier familia finita $M_1, \ldots, M_n$ de A-módulos, obteniéndose un A-módulo $M_1 \otimes_A \cdots \otimes_A M_n$ con una propiedad universal similar. Para definir un morfismo de A-módulos $f\colon M_1 \otimes_A \cdots \otimes_A M_n \to P$, bastará definir las imágenes $f(m_1 \otimes \cdots \otimes m_n)$ de modo que

$$f(m_1 \otimes \cdots \otimes a_i m_i + n_i \otimes \cdots) = a_i f(m_1 \otimes \cdots \otimes m_i \otimes \cdots) + f(m_1 \otimes \cdots \otimes n_i \otimes \cdots)$$

5. Teorema : *Existen isomorfismos naturales*

1. $(M \otimes_A N) \otimes_A P = M \otimes_A (N \otimes_A P)$, $(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)$.
2. $M \otimes_A N = N \otimes_A M$, $m \otimes n \mapsto n \otimes m$.
3. $A \otimes_A M = M$, $a \otimes m \mapsto am$.
4. $(\bigoplus_i M_i) \otimes_A N = \bigoplus_i (M_i \otimes N)$, $(m_i) \otimes n \mapsto (m_i \otimes n)$.
5. $M \otimes_A A/I = M/IM$, $m \otimes \bar{a} \mapsto \overline{am}$.

Demostración. Dejamos al lector que defina los morfismos inversos. Veamos, sólo, que el morfismo de 1. está bien definido: Para cada p el morfismo $M \otimes_A N \times p \to M \otimes_A (N \otimes_A P)$, $(m \otimes n) \times p \mapsto m \otimes (n \otimes p)$ está bien definido. Luego tenemos un morfismo $(M \otimes_A N) \times P \to M \otimes_A (N \otimes_A P)$, que es bilineal e induce el morfismo definido en 1. □

6. Definición : Si $f\colon A \to B$ es un morfismo de anillos, se dice que B es una A-álgebra. Usualmente denotaremos $f(a) = a$.

Sea B una A-álgebra y N un B-módulo. Entonces, N es de modo natural un A-módulo: $a \cdot n := f(a) \cdot n$, para todo $a \in A$ y $n \in N$. Sea M un A-módulo y N un B-módulo. Cada elemento $b \in B$ define un endomorfismo $1 \otimes b\colon M \otimes_A N \to M \otimes_A N$, $m \otimes n \underset{\text{def}}{\mapsto} m \otimes bn$. Podemos definir así, una estructura de B-módulo en $M \otimes_A N$ que viene dada por el siguiente producto

$$b \cdot (\sum_i m_i \otimes n_i) := \sum_i m_i \otimes bn_i$$

7. Teorema: *Sea $A \to B$ un morfismo de anillos, M un A-módulo y N, P dos B-módulos. Existen isomorfismos naturales*

1. $\mathrm{Hom}_B(M \otimes_A N, P) = \mathrm{Hom}_A(M, \mathrm{Hom}_B(N, P))$.
2. $(M \otimes_A N) \otimes_B P = M \otimes_A (N \otimes_B P)$, $(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)$.

Demostración. 1. Basta comprobar que vía la igualdad $\mathrm{Hom}_A(M \otimes_A N, P) = \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$, el submódulo $\mathrm{Hom}_B(M \otimes_A N, P)$ se corresponde con el submódulo $\mathrm{Hom}_A(M, \mathrm{Hom}_B(N, P))$. El resto al lector. □

Sea $f\colon A \to B$ un morfismo de anillos. Se dice que $M \otimes_A B$ es el cambio de base de M por $A \to B$.

Notación: Denotaremos $M \otimes_A B = M_B$.

8. Proposición: *Sean $A \to B$ y $B \to C$ morfismos de anillos, M y M' A-módulos y N un B-módulo. Existen isomorfismos naturales*

1. $M_B \otimes_B N = M \otimes_A N$, $(m \otimes b) \otimes n \mapsto m \otimes bn$.
2. $(M \otimes_A M') \otimes_A B = M_B \otimes_B M'_B$, $(m \otimes m') \otimes b \mapsto (m \otimes b) \otimes (m' \otimes 1)$. *En particular, dado un sistema multiplicativo $S \subset A$, $(M \otimes_A N)_S = M_S \otimes_{A_S} N_S$.*
3. $(M_B)_C = M_C$, *(i.e., $(M \otimes_A B) \otimes_B C = M \otimes_A C$, $(m \otimes b) \otimes c \mapsto m \otimes bc$).*

Demostración. Defínanse los morfismos inversos. □

1.4. Producto tensorial de álgebras

Ahora, nuestro objetivo es definir el producto tensorial de A-álgebras.

1. Definición: Dadas dos A-álgebras B y C, diremos que un morfismo de anillos $\phi\colon B \to C$ es un morfismo de A-álgebras si $\phi(a) = a$, para todo $a \in A$. Denotaremos $\mathrm{Hom}_{A-alg}(B, C)$ al conjunto de todos los morfismos de A-álgebras de B en C.

2. Ejemplo: $\mathbb{C}$ es una $\mathbb{R}$-álgebra del modo obvio. Dado un anillo A, $A[x_1, \ldots, x_n]$ es una A-álgebra: $A \to A[x_1, \ldots, x_n]$, $a \mapsto a$.

3. Ejercicio: Calcular $\mathrm{Hom}_{A-alg}(A[x_1, \ldots, x_n], B)$.

Si B y C son A-álgebras, el A-módulo $B \otimes_A C$ tiene una estructura de A-álgebra natural: El producto es el morfismo $B \otimes_A C \times B \otimes_A C \to B \otimes_A C$, $(b \otimes c, b' \otimes c') \mapsto bb' \otimes cc'$ inducido por el correspondiente morfismo $B \otimes_A C \otimes B \otimes_A C \to B \otimes_A C$. Con este producto $B \otimes_A C$ es un anillo. Por último, el morfismo $A \to B \otimes_A C$, $a \mapsto a \otimes 1 = 1 \otimes a$ es un morfismo de anillos.

4. Proposición: *Sean B, C y D A-álgebras. Se cumple el isomorfismo*

$$\begin{array}{ccc} \mathrm{Hom}_{A-alg}(B \otimes_A C, D) & = & \mathrm{Hom}_{A-alg}(B, D) \times \mathrm{Hom}_{A-alg}(C, D) \\ \phi & \longmapsto & (\phi_1, \phi_2) \ \ \phi_1(b) := \phi(b \otimes 1), \phi_2(c) := \phi(1 \otimes c) \\ \phi\colon (b \otimes c) \mapsto \phi_1(b)\phi_2(c) & \longmapsfrom & (\phi_1, \phi_2) \end{array}$$

5. Proposición: *Sean B y C A-álgebras. Se cumple el isomorfismo*

$$\begin{aligned} \mathrm{Hom}_A(B,C) &\longrightarrow \mathrm{Hom}_C(B_C,C) \\ \phi &\longmapsto \phi' : \phi'(b\otimes c) = \phi(b)\cdot c \\ \phi'_{|B} &\longleftarrow \phi' \end{aligned}$$

1.5. Biografía de Gauss

GAUSS BIOGRAPHY

At the age of seven, Carl Friedrich Gauss started elementary school, and his potential was noticed almost immediately. His teacher, Büttner, and his assistant, Martin Bartels, were amazed when Gauss summed the integers from 1 to 100 instantly by spotting that the sum was 50 pairs of numbers each pair summing to 101.
In 1788 Gauss began his education at the Gymnasium with the help of Büttner and Bartels, where he learnt High German and Latin. After receiving a stipend from the Duke of Brunswick- Wolfenbüttel, Gauss entered Brunswick Collegium Carolinum in 1792. At the academy Gauss independently discovered Bode's law, the binomial theorem and the arithmetic-geometric mean, as well as the law of quadratic reciprocity and the prime number theorem.

In 1795 Gauss left Brunswick to study at Göttingen University. Gauss's teacher there was Kästner, whom Gauss often ridiculed. His only known friend amongst the students was Farkas Bolyai. They met in 1799 and corresponded with each other for many years.

Gauss left Göttingen in 1798 without a diploma, but by this time he had made one of his most important discoveries - the construction of a regular 17-gon by ruler and compasses This was the most major advance in this field since the time of Greek mathematics and was published as Section VII of Gauss's famous work, Disquisitiones Arithmeticae.

Gauss returned to Brunswick where he received a degree in 1799. After the Duke of Brunswick had agreed to continue Gauss's stipend, he requested that Gauss submit a doctoral dissertation to the University of Helmstedt. He already knew Pfaff, who was chosen to be his advisor. Gauss's dissertation was a discussion of the fundamental theorem of algebra.

With his stipend to support him, Gauss did not need to find a job so devoted himself to research. He published the book Disquisitiones Arithmeticae in the summer of 1801. There were seven sections, all but the last section, referred to above, being devoted to number theory.

In June 1801, Zach, an astronomer whom Gauss had come to know two or three years previously, published the orbital positions of Ceres, a new "small planet"which was discovered by G Piazzi, an Italian astronomer on 1 January, 1801. Unfortunately, Piazzi had only been able to observe 9 degrees of its orbit before it disappeared behind the Sun. Zach published several predictions of its position, including one by Gauss which differed greatly from the others. When Ceres was rediscovered by Zach on 7 December 1801 it was almost exactly where Gauss had predicted. Although he did not disclose his methods at the time, Gauss had used his least squares approximation method.

In June 1802 Gauss visited Olbers who had discovered Pallas in March of that year and Gauss investigated its orbit. Olbers requested that Gauss be made director of the proposed new observatory in Göttingen, but no

action was taken. Gauss began corresponding with Bessel, whom he did not meet until 1825, and with Sophie Germain.

Gauss married Johanna Ostoff on 9 October, 1805. Despite having a happy personal life for the first time, his benefactor, the Duke of Brunswick, was killed fighting for the Prussian army. In 1807 Gauss left Brunswick to take up the position of director of the Göttingen observatory.

Gauss arrived in Göttingen in late 1807. In 1808 his father died, and a year later Gauss's wife Johanna died after giving birth to their second son, who was to die soon after her. Gauss was shattered and wrote to Olbers asking him to give him a home for a few weeks,

to gather new strength in the arms of your friendship - strength for a life which is only valuable because it belongs to my three small children.

Gauss was married for a second time the next year, to Minna the best friend of Johanna, and although they had three children, this marriage seemed to be one of convenience for Gauss.

Gauss's work never seemed to suffer from his personal tragedy. He published his second book, Theoria motus corporum coelestium in sectionibus conicis Solem ambientium, in 1809, a major two volume treatise on the motion of celestial bodies. In the first volume he discussed differential equations, conic sections and elliptic orbits, while in the second volume, the main part of the work, he showed how to estimate and then to refine the estimation of a planet's orbit. Gauss's contributions to theoretical astronomy stopped after 1817, although he went on making observations until the age of 70.

Much of Gauss's time was spent on a new observatory, completed in 1816, but he still found the time to work on other subjects. His publications during this time include Disquisitiones generales circa seriem infinitam, a rigorous treatment of series and an introduction of the hypergeometric function, Methodus nova integralium valores per approximationem inveniendi, a practical essay on approximate integration, Bestimmung der Genauigkeit der Beobachtungen, a discussion of statistical estimators, and Theoria attractionis corporum sphaeroidicorum ellipticorum homogeneorum methodus nova tractata. The latter work was inspired by geodesic problems and was principally concerned with potential theory. In fact, Gauss found himself more and more interested in geodesy in the 1820s.

Gauss had been asked in 1818 to carry out a geodesic survey of the state of Hanover to link up with the existing Danish grid. Gauss was pleased to accept and took personal charge of the survey, making measurements during the day and reducing them at night, using his extraordinary mental capacity for calculations. He regularly wrote to Schumacher, Olbers and Bessel, reporting on his progress and discussing problems.

Because of the survey, Gauss invented the heliotrope which worked by reflecting the Sun's rays using a design of mirrors and a small telescope. However, inaccurate base lines were used for the survey and an unsatisfactory network of triangles. Gauss often wondered if he would have been better advised to have pursued some other occupation but he published over 70 papers between 1820 and 1830.

In 1822 Gauss won the Copenhagen University Prize with Theoria attractionis... together with the idea of mapping one surface onto another so that the two are similar in their smallest parts. This paper was published in 1825 and led to the much later publication of Untersuchungen über Gegenstände der Höheren Geodäsie (1843 and 1846). The paper Theoria combinationis observationum erroribus minimis obnoxiae (1823), with its supplement (1828), was devoted to mathematical statistics, in particular to the least squares method.

From the early 1800s Gauss had an interest in the question of the possible existence of a non-Euclidean geometry. He discussed this topic at length with Farkas Bolyai and in his correspondence with Gerling and Schumacher. In a book review in 1816 he discussed proofs which deduced the axiom of parallels from the other Euclidean axioms, suggesting that he believed in the existence of non-Euclidean geometry, although he was rather vague.

... the vain effort to conceal with an untenable tissue of pseudo proofs the gap which one cannot fill out.

Gauss confided in Schumacher, telling him that he believed his reputation would suffer if he admitted in public that he believed in the existence of such a geometry.

In 1831 Farkas Bolyai sent to Gauss his son János Bolyai's work on the subject. Gauss replied

to praise it would mean to praise myself.

Again, a decade later, when he was informed of Lobachevsky's work on the subject, he praised its "genuinely geometricçharacter, while in a letter to Schumacher in 1846, states that he

had the same convictions for 54 years

indicating that he had known of the existence of a non-Euclidean geometry since he was 15 years of age (this seems unlikely).

Gauss had a major interest in differential geometry, and published many papers on the subject. Disquisitiones generales circa superficies curva (1828) was his most renowned work in this field. In fact, this paper rose from his geodesic interests, but it contained such geometrical ideas as Gaussian curvature. The paper also includes Gauss's famous theorema egregrium:

If an area in E^3 can be developed (i.e. mapped isometrically) into another area of E^3, the values of the Gaussian curvatures are identical in corresponding points.

The period 1817-1832 was a particularly distressing time for Gauss. He took in his sick mother in 1817, who stayed until her death in 1839, while he was arguing with his wife and her family about whether they should go to Berlin. He had been offered a position at Berlin University and Minna and her family were keen to move there. Gauss, however, never liked change and decided to stay in Göttingen. In 1831 Gauss's second wife died after a long illness.

In 1831, Wilhelm Weber arrived in Göttingen as physics professor filling Tobias Mayer's chair. Gauss had known Weber since 1828 and supported his appointment. Gauss had worked on physics before 1831, publishing Über ein neues allgemeines Grundgesetz der Mechanik, which contained the principle of least constraint, and Principia generalia theoriae figurae fluidorum in statu aequilibrii which discussed forces of attraction. These papers were based on Gauss's potential theory, which proved of great importance in his work on physics. He later came to believe his potential theory and his method of least squares provided vital links between science and nature.

In 1832, Gauss and Weber began investigating the theory of terrestrial magnetism after Alexander von Humboldt attempted to obtain Gauss's assistance in making a grid of magnetic observation points around the Earth. Gauss was excited by this prospect and by 1840 he had written three important papers on the subject: Intensitas vis magneticae terrestris ad mensuram absolutam revocata (1832), Allgemeine Theorie des Erdmagnetismus (1839) and Allgemeine Lehrsätze in Beziehung auf die im verkehrten Verhältnisse des Quadrats der Entfernung wirkenden Anziehungs- und Abstossungskräfte (1840). These papers all dealt with the current theories on terrestrial magnetism, including Poisson's ideas, absolute measure for magnetic force and an empirical definition of terrestrial magnetism. Dirichlet's principle was mentioned without proof.

Allgemeine Theorie... showed that there can only be two poles in the globe and went on to prove an important theorem, which concerned the determination of the intensity of the horizontal component of the magnetic force along with the angle of inclination. Gauss used the Laplace equation to aid him with his calculations, and ended up specifying a location for the magnetic South pole.

Humboldt had devised a calendar for observations of magnetic declination. However, once Gauss's new magnetic observatory (completed in 1833 - free of all magnetic metals) had been built, he proceeded to alter many of Humboldt's procedures, not pleasing Humboldt greatly. However, Gauss's changes obtained more accurate results with less effort.

Gauss and Weber achieved much in their six years together. They discovered Kirchhoff's laws, as well as building a primitive telegraph device which could send messages over a distance of 5000 ft. However, this was just an enjoyable pastime for Gauss. He was more interested in the task of establishing a world-wide net of

magnetic observation points. This occupation produced many concrete results. The Magnetischer Verein and its journal were founded, and the atlas of geomagnetism was published, while Gauss and Weber's own journal in which their results were published ran from 1836 to 1841.

In 1837, Weber was forced to leave Göttingen when he became involved in a political dispute and, from this time, Gauss's activity gradually decreased. He still produced letters in response to fellow scientists' discoveries usually remarking that he had known the methods for years but had never felt the need to publish. Sometimes he seemed extremely pleased with advances made by other mathematicians, particularly that of Eisenstein and of Lobachevsky.

Gauss spent the years from 1845 to 1851 updating the Göttingen University widow's fund. This work gave him practical experience in financial matters, and he went on to make his fortune through shrewd investments in bonds issued by private companies.

Two of Gauss's last doctoral students were Moritz Cantor and Dedekind. Dedekind wrote a fine description of his supervisor

... usually he sat in a comfortable attitude, looking down, slightly stooped, with hands folded above his lap. He spoke quite freely, very clearly, simply and plainly: but when he wanted to emphasise a new viewpoint ... then he lifted his head, turned to one of those sitting next to him, and gazed at him with his beautiful, penetrating blue eyes during the emphatic speech. ... If he proceeded from an explanation of principles to the development of mathematical formulas, then he got up, and in a stately very upright posture he wrote on a blackboard beside him in his peculiarly beautiful handwriting: he always succeeded through economy and deliberate arrangement in making do with a rather small space. For numerical examples, on whose careful completion he placed special value, he brought along the requisite data on little slips of paper.

Gauss presented his golden jubilee lecture in 1849, fifty years after his diploma had been granted by Helmstedt University. It was appropriately a variation on his dissertation of 1799. From the mathematical community only Jacobi and Dirichlet were present, but Gauss received many messages and honours.

From 1850 onwards Gauss's work was again nearly all of a practical nature although he did approve Riemann's doctoral thesis and heard his probationary lecture. His last known scientific exchange was with Gerling. He discussed a modified Foucault pendulum in 1854. He was also able to attend the opening of the new railway link between Hanover and Göttingen, but this proved to be his last outing. His health deteriorated slowly, and Gauss died in his sleep early in the morning of 23 February, 1855.

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/)

1.6. Problemas

1. Dar ejemplos que muestren que

   a) La intersección de ideales primos no siempre es un ideal primo.

   b) La unión de ideales no siempre es un ideal.

   c) La imagen de un ideal por un morfismo de anillos no siempre es un ideal.

2. Probar que $(x_1 - a_1, \ldots, x_n - a_n)$ es un ideal maximal del anillo $k[x_1, \ldots, x_n]$, formado por todos los polinomios $p(x_1, \ldots, x_n)$ tales que $p(a_1, \ldots, a_n) = 0$, y que

$$k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n) \;=\; k$$

3. Si $\mathfrak{m}$ es un ideal maximal de $k[x_1, \ldots, x_n]$ tal que $k = k[x_1, \ldots, x_n]/\mathfrak{m}$. Probar que existen $a_1, \ldots, a_n \in k$ tales que $\mathfrak{m} = (x - a_1, \ldots, x - a_n)$.

4. Sea $I = (p_1, \ldots, p_r)$ un ideal de un anillo de polinomios $A = k[x_1, \ldots, x_n]$ con coeficientes en un cuerpo k. Probar que la condición necesaria y suficiente para que $I \neq A$ es que el sistema de ecuaciones

$$\begin{aligned} p_1(x_1, \ldots, x_n) &= 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots & \\ p_r(x_1, \ldots, x_n) &= 0 \end{aligned}$$

admita alguna solución $x_1 = \alpha_1, \ldots, x_n = \alpha_n$ en alguna extensión L de k.

5. Sea A un anillo y $f, g \in A$. Probar que $(g)_0 \subseteq (f)_0 \Leftrightarrow g$ divide a alguna potencia de f.

6. Sea $\mathfrak{a}$ un ideal de un anillo A. Probar que la condición necesaria y suficiente para que $(\mathfrak{a})_0 = \operatorname{Spec} A$ es que el ideal $\mathfrak{a}$ esté generado por elementos nilpotentes.

7. Probar que el núcleo del morfismo de localización $A \to A_S$ es el ideal
$$\{a \in A\colon\ sa = 0 \text{ para algún } s \in S\}.$$

8. Dar un ejemplo en que el morfismo de localización $A \to A_S$ no sea inyectivo.

9. ¿Es cierto que el cuerpo de fracciones de $\mathbb{Z}[x]$ es isomorfo a $\mathbb{Q}(x)$?
Si $\alpha \in \mathbb{C}$, ¿es cierto que el cuerpo de fracciones de $\mathbb{Z}[\alpha]$ es isomorfo a $\mathbb{Q}(\alpha)$?

10. Dado un morfismo de anillos $f\colon A \to B$ y un sistema multiplicativo $S \subset A$, denotaremos a $f(S)$ simplemente por S. Si $S, S' \subset A$ son dos sistemas multiplicativos, denotemos $S \cdot S' = \{ss'\colon\ s \in S, s' \in S'\}$. Probar

   a) $B \otimes_A A_S = B_S$.

   b) $(A_S)_{S'} = A_{S \cdot S'}$.

11. Dado un ideal $I \subset A$ y un A-módulo M, denotemos $I \cdot M := \{\sum_{j=1}^{n} i_j \cdot m_j : \text{con } i_j \in I, m_j \in M, n \in \mathbb{N}\}$. Si J es un ideal del anillo A_S, probar que existe un ideal I de A tal que $J = I \cdot A_S$.

12. Si $\mathfrak{p}$ es un ideal primo del anillo A y $\mathfrak{p} \cap S = \emptyset$, probar que $\mathfrak{p} \cdot A_S$ es un ideal primo de A_S.

13. Sea $i\colon A \to A_S$ el morfismo de localización. Probar que

$$\operatorname{Spec} A_S \overset{i^*}{=} \{x \in \operatorname{Spec} A\colon\ \mathfrak{p}_x \cap S = \emptyset\}$$

14. Probar que si M y N son A-módulos libres entonces $M \otimes_A N$ es un A-módulo libre. Probar que si $\{m_i\}_{i\in I}$ y $\{n_j\}_{j\in J}$ son bases de dos A-módulos libres M y N, probar que $\{m_i \otimes n_j\}_{(i,j)\in I\times J}$ es una base del A-módulo libre $M \otimes_A N$.

15. Sea $A \to B$ un morfismo de anillos. Probar que si $\{m_i\}_{i\in I}$ es un sistema de generadores de un A-módulo M, entonces $\{m_i \otimes 1\}_{i\in I}$ es un sistema de generadores del B-módulo $M \otimes_A B$. Además, si $\{e_i\}_{i\in I}$ es una base de un A-módulo libre L, probar que $\{e_i \otimes 1\}_{i\in I}$ es una base del B-módulo libre $L \otimes_A B$.

16. Si E es un k-espacio vectorial y L es una extensión de k, entonces $\dim_L(E \otimes_k L) = \dim_k E$.

17. Sea $\{e_1, \ldots, e_n\}$ una base de un k-espacio vectorial E. Si $(x_1, \ldots, x_n)$ son las coordenadas de un vector $e \in E$ en tal base, determinar las coordenadas de $e \otimes 1 \in E \otimes_k L$ en la base $\{e_1 \otimes 1, \ldots, e_n \otimes 1\}$

18. Sea $f\colon E \to E'$ una aplicación lineal entre dos k-espacios vectoriales. Si $A = (a_{ij})$ es la matriz de f en sendas bases $\{e_1, \ldots, e_n\}$ y $\{e'_1, \ldots, e'_m\}$ de E y E', determinar la matriz de $f \otimes \mathrm{Id}\colon E \otimes_k L \to E' \otimes_k L$ en las bases $\{e_1 \otimes 1, \ldots, e_n \otimes 1\}$ y $\{e'_1 \otimes 1, \ldots, e'_m \otimes 1\}$.

19. Probar que si $0 \to M_1 \to M_2 \to M_3 \to 0$ es una sucesión exacta de A-módulos y N es un A-módulo libre, entonces
$$0 \to M_1 \otimes_A N \to M_2 \otimes_A N \to M_3 \otimes_A N \to 0$$
es una sucesión exacta de A-módulos.

20. Probar que si $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ es una sucesión exacta de A-módulos y N es un A-módulo, entonces
$$M_1 \otimes_A N \xrightarrow{f\otimes \mathrm{Id}} M_2 \otimes_A N \xrightarrow{g\otimes \mathrm{Id}} M_3 \otimes_A N \to 0$$
es una sucesión exacta de A-módulos.

21. Sea E' un subespacio vectorial de un k-espacio vectorial E. Para todo k-espacio vectorial V, probar que $(E/E') \otimes_k V = (E \otimes_k V)/(E' \otimes_k V)$.

22. Sea $f\colon E' \to E$ una aplicación k-lineal, V un k-espacio vectorial y consideremos la aplicación lineal $f \otimes 1\colon E' \otimes_k V \to E \otimes_k V$. Probar que $\mathrm{Im}(f \otimes \mathrm{Id}) = (\mathrm{Im}\, f) \otimes_k V$ y $\mathrm{Ker}(f \otimes \mathrm{Id}) = (\mathrm{Ker}\, f) \otimes_k V$.

23. Sea A una k-álgebra finita y $a \in A$. Probar que $a \in k$ si y sólo si $a \otimes 1 = 1 \otimes a$ en $A \otimes_k A$.
(*Indicación:* Considerar una base de A sobre k y la correspondiente base de $A \otimes_k A$).

24. Sea $A \to B$ un morfismo de anillos. Probar que $A[x_1, \ldots, x_n] \otimes_A B = B[x_1, \ldots, x_n]$.

25. Sea $A \to B$ un morfismo de anillos. Probar que
$$(A[x_1, \ldots, x_n]/(p_1, \ldots, p_r)) \otimes_A B \;=\; B[x_1, \ldots, x_n]/(p_1, \ldots, p_r)\,.$$
(los polinomios con coeficientes en A, vía el morfismo $A \to B$ los consideramos como polinomios con coeficientes en B)

26. Probar que $(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z}) \;=\; \mathbb{Z}/d\mathbb{Z}$, donde $d = \text{m.c.d.}(m, n)$.

27. Probar que $A/I \otimes_A A/J = A/(I + J)$.

28. Sean I y J dos ideales de un anillo A. Si $I + J = A$, demostrar que para todo A-módulo M, tenemos un isomorfismo natural $M/IJM \;=\; (M/IM) \oplus (M/JM)$.

29. Si $T^q_p(E)$ denota el espacio vectorial de los tensores de tipo (p, q) sobre un k-espacio vectorial de dimensión finita, probar la existencia de un isomorfismo natural
$$T^q_p(E) = E^* \otimes_k \overset{p}{\ldots} \otimes_k E^* \otimes_k E \otimes_k \overset{q}{\ldots} \otimes_k E\,.$$

30. Si E y F son k-espacios vectoriales y $\dim_k E < \infty$, probar que $\mathrm{Hom}_k(E, F) = E^* \otimes_k F$.

Capítulo 2

Raíces de un polinomio. Extensiones finitas de cuerpos

2.1. Extensiones de cuerpos

1. Definición : Una extensión de cuerpos es un morfismo de anillos $k \to K$, donde k y K son cuerpos. También se dice que K es una extensión de cuerpos de k. Obsérvese que todo morfismo (de anillos) entre cuerpos es inyectivo pues el núcleo es un ideal, que ha de ser el ideal (0) y no el ideal $k = (1)$, porque el elemento unidad se aplica en el elemento unidad.

2. Proposición: *La k-álgebra $A = k[x]/(x^n+a_1x^{n-1}+\ldots+a_n)$ es un k-espacio vectorial de base $\{1, \bar{x}, \ldots, \bar{x}^{n-1}\}$.:*

Demostración. Sea $q(x) = x^n + a_1x^{n-1} + \ldots + a_n$. Dado un polinomio $p(x)$ existen dos polinomios únicos $c(x)$ y $r(x)$, de modo que $p(x) = c(x) \cdot q(x) + r(x)$ y que $\operatorname{gr} r(x) < \operatorname{gr} q(x)$. Es decir, existe un único polinomio $r(x)$ de grado menor que n de modo que $\overline{r(x)} = \overline{p(x)}$ en $k[x]/(q(x))$.

Es decir, la aplicación $k \oplus k \cdot x \oplus \cdots \oplus k \cdot x^{n-1} \to k[x]/(q(x))$, $r(x) \mapsto \overline{r(x)}$ es un isomorfismo.

□

3. Definición : Diremos que una extensión de cuerpos $k \hookrightarrow K$ es una extensión finita de cuerpos si K es un k-espacio vectorial de dimensión finita. Llamaremos grado de K sobre k a $\dim_k K$.

4. Ejemplo : Por ejemplo, la inclusión $\mathbb{R} \subset \mathbb{C}$ es una extensión finita de cuerpos de grado 2, la inclusión $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[x]/(x^2 - 2)$ también.

5. Ejercicio : Calcular $(1 + 5\sqrt{2}) \cdot (1 - 3\sqrt{2})$ y $\frac{1}{1+5\sqrt{2}}$.

6. Proposición : *Si $k \to K$ es una extensión finita de cuerpos de grado n y $K \to \Sigma$ es una extensión finita de grado m, entonces $k \to \Sigma$ es una extensión finita de grado $n \cdot m$. En particular, la composición de extensiones finitas es una extensión finita.*

Demostración. Se tienen igualdades de espacios vectoriales $\Sigma = K\oplus\overset{m}{\ldots}\oplus K$, y $K = k\oplus\overset{n}{\ldots}\oplus k$, luego $\Sigma = k\oplus\overset{n\cdot m}{\ldots}\oplus k$ y se concluye. □

Sean dos extensiones de cuerpos $k \hookrightarrow K$ y $k \hookrightarrow K'$ y sea $\mathfrak{m} \subset K \otimes_k K'$ un ideal maximal. Denotaremos $K \cdot K' := (K \otimes_k K')/\mathfrak{m}$ y diremos que es un compuesto de K y K'. Observemos que tenemos morfismos naturales $K \to K \otimes_k K' \to K \cdot K'$ y $K' \to K \otimes_k K' \to K \cdot K'$ y la mínima k-subextensión de $K \cdot K'$ que contiene a K y K'

es $K \cdot K'$. Si K y K' son extensiones finitas de grados n y n', entonces $K \cdot K'$ es una extensión finita de grado menor o igual que $n \cdot n'$.

Sea $k \hookrightarrow K$ una extensión de cuerpos. Dados $\alpha_1, \ldots, \alpha_n \in K$, denotamos $k(\alpha_1, \ldots, \alpha_n)$ a la mínima subextensión de K que contiene a $\alpha_1, \ldots, \alpha_n$. Explícitamente,

$$k(\alpha_1, \ldots, \alpha_n) = \{\frac{p(\alpha_1, \ldots, \alpha_n)}{q(\alpha_1, \ldots, \alpha_n)} \in K\colon\ p(x_1, \ldots, x_n), q(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] \text{ y } q(\alpha_1, \ldots, \alpha_n) \neq 0\}$$

2.2. Teorema de Kronecker

1. Teorema de Kronecker: *Sea $p(x) \in k[x]$ un polinomio de grado $n > 0$. Existe una extensión finita K de k en la que $p(x)$ descompone en factores simples, es decir, existen $\alpha_1, \ldots, \alpha_n \in K$ tales que*

$$p(x) = \lambda \cdot (x - \alpha_1) \cdots (x - \alpha_n), \qquad \lambda \in k$$

Si K' es otra extensión de cuerpos k y $\beta \in K'$ es una raíz de $p(x)$, entonces en todo compuesto $K \cdot K'$ se cumple que $\beta = \alpha_i$, para algún i. Si $\beta_1, \ldots, \beta_n \in K'$ son tales que $p(x) = \lambda \cdot (x - \beta_1) \cdots (x - \beta_n)$, entonces en $K \cdot K'$ se tiene que $\alpha_i = \beta_i$, para todo i (reordenando las β_i si es necesario). Se dice que $\alpha_1, \ldots, \alpha_n$ son las raíces de $p(x)$.

Demostración. Procedamos por inducción sobre n. Si $n = 1$, basta tomar $K = k$, pues $p(x) = \lambda(x - \alpha)$, con $\alpha \in k$. Supongamos que $n > 1$. Sea $p_1(x) \in k[x]$ un polinomio irreducible que divida a $p(x)$. Sea $K = k[x]/(p_1(x))$ y denotemos $\bar{x} = \alpha_1$. Obviamente, $p_1(\alpha_1) = 0$, luego $p(\alpha_1) = 0$. Por tanto, en $K[x]$ tenemos que $p(x) = (x - \alpha_1) \cdot p_2(x)$. Por hipótesis de inducción, existe una extensión finita $K \hookrightarrow K'$ de modo que $p_2(x) = \lambda \cdot (x - \alpha_2) \cdots (x - \alpha_n)$. Luego en K', que es una extensión finita de k,

$$p(x) = \lambda \cdot (x - \alpha_1) \cdots (x - \alpha_n)$$

En $K \cdot K'$, $0 = p(\beta) = \lambda \cdot (\beta - \alpha_1) \cdots (\beta - \alpha_n)$, luego $\beta = \alpha_i$, para algún i.

Si $p(x) = \lambda \cdot (x - \beta_1) \cdots (x - \beta_n)$ (en $K \cdot K'$), como $0 = p(\alpha_1) = \lambda \cdot (\alpha_1 - \beta_1) \cdots (\alpha_1 - \beta_n)$, reordenando las β_i, podemos suponer que $\beta_1 = \alpha_1$. Dividiendo por $x - \alpha_1$, tendremos que $\lambda \cdot (x - \beta_2) \cdots (x - \beta_n) = \lambda \cdot (x - \alpha_2) \cdots (x - \alpha_n)$. Por inducción sobre n, reordenado $\beta_2, \ldots, \beta_n$, tendremos que $\beta_i = \alpha_i$, para todo $i \geq 2$.

□

2. Observación : Agrupando los factores simples con la misma raíz, tenemos (en $K[x]$) que

$$p(x) = \lambda \cdot (x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r}, \quad \text{con } \alpha_i \neq \alpha_j \text{ para todo } i \neq j$$

Si $n_i > 1$, se dice que α_i es una raíz múltiple de $p(x)$ de multiplicidad n_i.

3. Proposición: *Sea $p(x) \in k[x]$ un polinomio no nulo y K una extensión de cuerpos de k. Entonces, $\alpha \in K$ es una raíz múltiple de $p(x)$ si y sólo si es raíz de $p(x)$ y $p'(x)$ (la derivada "formal" de $p(x)$).*

Demostración. Tenemos que α es una raíz de $p(x)$, entonces $p(x) = (x - \alpha) \cdot q(x)$ (en $K[x]$) y $p'(x) = q(x) + (x - \alpha) \cdot q'(x)$. Por tanto, α es una raíz de $p'(x)$ si y sólo si es raíz de $q(x)$, es decir, si y sólo si α es una raíz múltiple de $p(x)$. □

4. Observación : El máximo común divisor de dos polinomios se puede calcular mediante el algoritmo de Euclides, por tanto, no cambia si hacemos un cambio de cuerpo base. Consideremos una extensión de cuerpos

K donde $p(x)$ y $q(x)$ descompongan es factores simples, podemos escribir $p(x) = \lambda \cdot (x-\alpha_1)^{n_1} \cdots (x-\alpha)^{n_r}$ y $q(x) = \mu \cdot (x-\alpha_1)^{m_1} \cdots (x-\alpha)^{m_r}$, con $n_i, m_i \geq 0$ y $\alpha_i \neq \alpha_j$, para todo $i \neq j$. Entonces

$$m.c.d(p(x), q(x)) = (x-\alpha_1)^{min(n_1,m_1)} \cdots (x-\alpha)^{min(n_r,m_r)} \in k[x]$$

Los polinomios $p(x)$ y $q(x)$ son primos entre sí si y sólo si no tienen raíces comunes (estamos considerando todas las raíces de $p(x)$ y $q(x)$ en K).

Un polinomio $p(x)$ no tiene raíces múltiples si y sólo si $p(x)$ y $p'(x)$ son primos entre sí.

5. Definición : Dado una extensión de cuerpos $k \hookrightarrow K$. Diremos que $\alpha \in K$ es algebraica sobre k si existe un polinomio $0 \neq p(x) \in k[x]$ tal que $p(\alpha) = 0$.

Si $\alpha \in K$ es algebraica entonces $k(\alpha) = k[x]/(p(x))$, donde $p(x)$ es el polinomio con coeficientes en k mínimo que anula a α. Por tanto, $\dim_k k(\alpha) = \text{gr}\, p(x) < \infty$ (véase 2.1.2). Recíprocamente, si $\dim_k k(\alpha) = n < \infty$ entonces $1, \alpha, \ldots, \alpha^n$ son k-linealmente dependientes, luego existe un polinomio de grado n que anula a α.

6. Definición : Se dice que una extensión de cuerpos $k \hookrightarrow K$ es algebraica si para cada elemento $\alpha \in K$ existe un polinomio $0 \neq p(x) \in k[x]$, de modo que $p(x) = 0$; es decir, para todo $\alpha \in K$, $k \to k(\alpha)$ es una extensión finita.

Si $k \to K$ es una extensión algebraica y $\alpha_1, \ldots, \alpha_n$ son elementos de K, entonces el cuerpo generado $k(\alpha_1, \ldots, \alpha_n)$ es una extensión finita de k, pues es composición de extensiones finitas $k \hookrightarrow k(\alpha_1) \hookrightarrow k(\alpha_1, \alpha_2) \hookrightarrow \cdots \hookrightarrow k(\alpha_1, \ldots, \alpha_n)$. Si $k \hookrightarrow K$ y $K \hookrightarrow K'$ son extensiones algebraicas entonces $k \hookrightarrow K'$ es algebraica: En efecto, dado $\alpha \in K'$, existe un polinomio $p(x) = \sum_i a_i x^i \in K[x]$ tal que $p(\alpha) = 0$. La extensión $k \hookrightarrow k(a_1, \ldots, a_n, \alpha)$ es finita, luego $k \hookrightarrow k(\alpha)$ también y concluimos.

7. Definición : Diremos que un cuerpo $\bar{k}$ es algebraicamente cerrado si no admite extensiones de cuerpos finitas (o algebraicas), es decir, todo polinomio con coeficientes en $\bar{k}$ tiene todas sus raíces en $\bar{k}$.

8. Teorema : *Dado un cuerpo k, existe una única extensión de cuerpos $k \hookrightarrow \bar{k}$, salvo isomorfismos, que es algebraica y tal que $\bar{k}$ es algebraicamente cerrado. Diremos que $\bar{k}$ es el cierre algebraico de k.*

Demostración. Sea P el conjunto de polinomios irreducibles de $k[x]$. Para cada $p \in P$ sea por Kronecker K_p un cuerpo que contenga a todas las raíces del polinomio p. Para cada subconjunto finito $\{p_1, \ldots, p_n\}$ de P consideremos la k-álgebra $K_{p_1} \otimes \ldots \otimes K_{p_n}$, y para cada inclusión $\{p_1, \ldots, p_n\} \subseteq \{p_1, \ldots, p_n, \ldots, p_m\}$ consideremos el morfismo obvio $K_{p_1} \otimes \ldots \otimes K_{p_n} \to K_{p_1} \otimes \ldots \otimes K_{p_n} \otimes \ldots \otimes K_{p_m}$. Sea A el límite inductivo de todos estos morfismos. Sea $\bar{k}$ el cociente de A por cualquier ideal maximal. Obviamente, $\bar{k}$ es una extensión algebraica de k, pues está generado algebraicamente por las imágenes de las extensiones K_p. Sea $\bar{k} \hookrightarrow K$ una extensión algebraica de cuerpos y $\alpha \in K$. K es una extensión algebraica de k, así pues α es algebraica sobre k. Sea $p = p(x) \in k[x]$ el polinomio mínimo anulador de α. K_p contiene todas las raíces de $p(x)$, luego $\bar{k}$ también, $\alpha \in \bar{k}$ y $K = \bar{k}$.

Si k' es una extensión algebraica de k, entonces $(\bar{k} \otimes_k k')/\mathfrak{m}$, siendo $\mathfrak{m}$ un ideal maximal, es una extensión algebraica de $\bar{k}$ y k'. Por tanto, $(\bar{k} \otimes_k k')/\mathfrak{m} = \bar{k}$ y ésta contiene a k'. Si k' es algebraicamente cerrado entonces $\bar{k} = k'$.

□

2.3. Teorema de las funciones simétricas. Teorema fundamental del Álgebra

Sea $P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = c(x-\alpha_1)\cdots(x-\alpha_n)$. Desarrollando el último término e igualando coeficientes de los x^i se obtiene las fórmulas de Cardano:

$$\begin{aligned} a_0 &= c \\ a_1 &= -c\cdot(\alpha_1+\cdots+\alpha_n) \\ &\cdots \\ a_i &= (-1)^i c\cdot \sum_{1\le j_1<\cdots<j_i\le n} \alpha_{j_1}\cdots\alpha_{j_i} \\ &\cdots \\ a_n &= (-1)^n c\cdot\alpha_1\cdots\alpha_n \end{aligned}$$

1. Definición : Llamaremos **funciones simétricas elementales** (o polinomios simétricos elementales) en las letras $x_1,\ldots,x_n$ a los polinomios $s_i \in \mathbb{Z}[x_1,\ldots,x_n]$ $(i=1,\ldots,n)$ definidos por:

$$\begin{aligned} s_1 &= x_1+\cdots+x_n \\ &\cdots \\ s_i &= \sum_{1\le j_1<\cdots<j_i\le n} x_{j_1}\cdots x_{j_i} \\ &\cdots \\ s_n &= x_1\cdots x_n \end{aligned}$$

Se cumple la igualdad:

$$\prod_i (x-x_i) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$$

Sea S_n el grupo de las permutaciones de n letras. Consideremos la operación de S_n en $A[x_1,\ldots x_n]$ siguiente:

$$\sigma(P(x_1,\ldots,x_n)) = P(x_{\sigma(1)},\ldots,x_{\sigma(n)})$$

para cada $\sigma\in S_n, P(x_1,\ldots,x_n)\in A[x_1,\ldots x_n]$.

2. Definición : Diremos que un polinomio $P(x_1,\ldots,x_n)\in A[x_1,\ldots x_n]$ es simétrico cuando $\sigma(P)=P$ para toda $\sigma\in S_n$. Al conjunto de las funciones simétricas las denotaremos $A[x_1,\ldots x_n]^{S_n}$.

3. Teorema de las funciones simétricas: *Se verifica la igualdad:*

$$A[x_1,\ldots,x_n]^{S_n} = A[s_1,\ldots,s_n]$$

Es decir, un polinomio en $x_1,\ldots,x_n$ con coeficientes en el anillo A es invariante por todas las permutaciones de las variables si y sólo si es un polinomio en las funciones simétricas elementales.

Demostración. Evidentemente todo polinomio en las funciones simétricas elementales es invariante por el grupo de las permutaciones. Por tanto, basta probar el recíproco.

Por inducción sobre el número n de variables. Sea $P(x_1,\ldots,x_n)\in A[x_1,\ldots,x_n]^{S_n}$. Descomponiendo P en sus componentes homogéneas, podemos suponer que P es homogéneo (de grado m) y vamos a probar que en

este caso existe $Q(y_1,\dots,y_n)$ tal que $P(x_1,\dots,x_n) = Q(s_1,\dots,s_n)$ y tal que Q es además casi homogéneo de grado m, es decir, es tal que $Q(ty_1,\dots,t^n y_n) = t^m Q(y_1,\dots,y_n)$. Para $n = 1$ es trivial.

Sea $P(x_1,\dots,x_n)$ un polinomio invariante homogéneo de grado m. Haciendo cociente por x_n se obtiene que $P(x_1,\dots,x_{n-1},0)$ es un polinomio homogéneo en $n-1$ variables e invariante por las permutaciones de éstas, luego $P(x_1,\dots,x_{n-1},0) = \overline{Q}(\overline{s}_1,\dots,\overline{s}_{n-1})$, siendo $\overline{s}_i$ la i-ésima función simétrica en las $i-1$ primeras variables, para cierto polinomio $\overline{Q}$ casi homogéneo de grado m. Sea $H(x_1,\dots,x_n) = P(x_1,\dots,x_n) - \overline{Q}(s_1,\dots,s_{n-1})$. Se verifica que H es simétrico y homogéneo de grado m y se anula para $x_n = 0$ (ya que $s_i = \overline{s}_i \, mod\, x_n$), luego es múltiplo de x_n y por ser simétrico es múltiplo de $x_1\cdots x_n = s_n$, es decir, $H(x_1,\dots,x_n) = s_n\cdot\overline{H}(x_1,\dots,x_n)$ y, por tanto, $\overline{H}(x_1,\dots,x_n)$ es simétrico también y homogéneo de grado $gr(\overline{H}) = gr(H)-n = gr(P)-n < gr(P)$, luego por recurrencia sobre el grado m de P se concluye que $\overline{H}(x_1,\dots,x_n) = \widetilde{Q}(s_1,\dots,s_n)$ con $\widetilde{Q}$ casi homogéneo de grado $m-n$. Sustituyendo en la definición de H y despejando se obtiene:

$$P(x_1,\dots x_n) = \overline{Q}(s_1,\dots,s_{n-1}) + s_n\cdot\widetilde{Q}(s_1,\dots,s_n)$$

con lo que se concluye. □

4. Corolario: *Sea k un cuerpo y $k(x_1,\dots,x_n)$ es el cuerpo de fracciones del anillo $k[x_1,\dots,x_n]$. Entonces, se verifica la igualdad:*

$$k(x_1,\dots,x_n)^{S_n} = k(s_1,\dots,s_n)$$

Demostración. Si $\frac{P}{Q}$ es una fracción irreducible (es decir, el numerador y denominador son primos entre sí) invariante por toda permutación, entonces $\frac{P}{Q} = \frac{\sigma(P)}{\sigma(Q)}$ para cada $\sigma\in S_n$, luego $\sigma(Q)P = \sigma(P)Q$. Como P, Q son primos entre sí se obtiene que $\sigma(P) = \lambda P$ y $\sigma(Q) = \lambda Q$. Ahora bien, de la igualdad $\sigma^{n!} = Id$ se concluye que $P = \sigma^{n!}(P) = \lambda^{n!}P$, luego $\lambda^{n!} = 1$ y, por tanto, $P^{n!}$ es invariante. Por ser $\frac{P}{Q} = \frac{P^{n!}}{QP^{n!-1}}$ invariante al igual que el numerador $P^{n!}$, se concluye que lo es también el denominador $QP^{n!-1}$. Es decir, $P^{n!}, QP^{n!-1}\in k[s_1,\dots,s_n]$ y, por tanto, $\frac{P}{Q} = \frac{P^{n!}}{QP^{n!-1}}\in k(s_1,\dots,s_n)$.

□

5. Teorema fundamental del Álgebra: *El cuerpo de los números complejos es un cuerpo algebraicamente cerrado.*

Demostración. Dado un polinomio cualquiera, $0\neq p(x)\in\mathbb{C}[x]$, tenemos que probar que tiene una raíz en $\mathbb{C}$. Basta probar que todo polinomio con coeficientes reales tiene una raíz compleja, porque el producto de $p(x)$ por su conjugado, $q(x) = p(x)\cdot\overline{p(x)}$ es un polinomio con coeficientes reales y si α es una raíz de $q(x)$, entonces α o su conjugada es una raíz de $p(x)$. Si $q(x)\in\mathbb{R}[x]$ es un polinomio de grado impar entonces

$$\lim_{x\to+\infty} q(x) = -\lim_{x\to-\infty} q(x),\quad (\text{y } |\lim_{x\to+\infty} q(x)| = +\infty)$$

Luego por el teorema de Bolzano existe un $\alpha\in\mathbb{R}$ tal que $q(\alpha) = 0$. Supongamos que $\operatorname{gr} q(x) = r = 2^n\cdot m$, con m impar. Para probar que $q(x)$ tiene una raíz compleja procedamos por inducción sobre n. Para $n = 0$ lo hemos probado. Supongamos $n > 0$. Sean $\alpha_1,\dots,\alpha_r$ las raíces de $q(x)$ y fijado $\lambda\in\mathbb{R}$ sean $\beta_{ij} := \alpha_i + \alpha_j + \lambda\alpha_i\cdot\alpha_j$. El polinomio $h(x) := \prod_{i<j}(x-\beta_{ij})\in\mathbb{R}[x]$, porque los coeficientes de $h(x)$ son funciones simétricas en $\alpha_1,\dots,\alpha_n$, luego por el teorema de las funciones simétricas, los coeficientes de $h(x)$ son polinomios en los coeficientes de $q(x)$. Observemos que $h(x)$ es un polinomio de grado $\binom{r}{2} = 2^{n-1}\cdot m'$ con m' impar. Por inducción sobre n, cierto $\beta_{rs} = \alpha_r + \alpha_s + \lambda\alpha_r\cdot\alpha_s\in\mathbb{C}$. Variando el λ fijado (tómese $\binom{r}{2}+1$ distintos), existirán $\lambda\neq\lambda'$ tales que

$$\alpha_r + \alpha_s + \lambda\alpha_r\cdot\alpha_s,\ \alpha_r + \alpha_s + \lambda'\alpha_r\cdot\alpha_s\in\mathbb{C}.$$

Luego $a := \alpha_r + \alpha_s$ y $b := \alpha_r\cdot\alpha_s\in\mathbb{C}$. Como α_r y α_s son las raíces de $(x-\alpha_r)(x-\alpha_s) = x^2 - ax + b$, tenemos que $\alpha_r, \alpha_s = (a\pm\sqrt{a^2-4b})/2\in\mathbb{C}$. □

2.4. Fórmulas de Newton y Girard

Sea $P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = a_0(x-\alpha_1)\cdots(x-\alpha_n) \in k[x]$.

1. Teorema: *Sea $P'(x)$ la derivada de $P(x)$ y $\sigma_i = \alpha_1^i + \cdots + \alpha_n^i$ las potencias simétricas en las raíces de $P(x)$. Se verifica:*

1. $$\left(\frac{P(x)}{x-\alpha_i}\right)(\alpha_i) = P'(\alpha_i)$$

2. *Si $\{\alpha_i\}_{i=1}^n \subset k$ son distintas, dados $\lambda_1, \ldots, \lambda_n \in k$ cualesquiera (eventualmente repetidos) el único polinomio $R(x)$ de grado menor que $n = gr\, P$ tal que $R(\alpha_i) = \lambda_i$ es el polinomio:*

$$R(x) = \sum_i \frac{\lambda_i}{P'(\alpha_i)} \frac{P(x)}{x-\alpha_i}$$

   (Fórmula de interpolación de Lagrange).

3. $$\frac{P'(x)}{P(x)} = \frac{1}{x-\alpha_1} + \cdots + \frac{1}{x-\alpha_n}$$

4. *Fórmula de Girard:*
$$\frac{P'(x)}{P(x)} = \frac{\sigma_0}{x} + \frac{\sigma_1}{x^2} + \cdots + \frac{\sigma_i}{x^{i+1}} + \cdots \in k[[\frac{1}{x}]]$$

5. *Fórmulas de Newton:*
$$\begin{aligned}
0 &= a_1 + \sigma_1 a_0 \\
0 &= 2a_2 + \sigma_1 a_1 + a_0\sigma_2 \\
0 &= 3a_3 + \sigma_1 a_2 + \sigma_2 a_1 + \sigma_3 a_3 \\
0 &= na_n + a_{n-1}\sigma_1 + \cdots + a_0\sigma_n \\
&\text{————————} \\
0 &= a_n\sigma_1 + \cdots + a_0\sigma_{n+1} \\
&\cdots \\
0 &= a_n\sigma_i + \cdots + a_0\sigma_{n+i} \\
&\cdots
\end{aligned}$$

Demostración. (1) Por el desarrollo de Taylor es $P(x) = P(\alpha) + P'(\alpha)(x-\alpha) + S(x)(x-\alpha)^2$ con $S(x) \in k[x]$, luego

$$\frac{P(x) - P(\alpha)}{x-\alpha} = P'(\alpha) + S(x)(x-\alpha)$$

Basta hacer $x = \alpha$.

(2) Por el apartado anterior, $H_i(x) = \frac{P(x)}{x-\alpha_i}$ es un polinomio de grado $n-1$ tal que $H_i(\alpha_i) = P'(\alpha_i)$ y $H_i(\alpha_j) = \frac{P(\alpha_j)}{\alpha_j - \alpha_i} = 0$, para todo $j \neq i$, de donde es fácil ver que el polinomio del enunciado es un polinomio de grado menor o igual que $n-1$ que toma los valores $R(\alpha_i) = \frac{\lambda_i}{P'(\alpha_i)} H_i(\alpha_i) = \lambda_i$.

La unicidad se obtiene de que si existiesen 2 la diferencia sería un polinomio no nulo de grado menor que n que se anula para $x = \alpha_i$, luego sería múltiplo de $\prod_i (x-\alpha_i)$ que es de grado n, lo cual es imposible.

(3) El polinomio $\sum_i \frac{P(x)}{x-\alpha_i}$ es de grado menor que n y toma el valor $\frac{P(x)}{x-\alpha_i}(\alpha_i) = P'(\alpha_i)$ para cada α_i, al igual que el polinomio $P'(x)$, luego coincide con él (por el apartado anterior).

(4) Sustituyendo $\frac{1}{x-\alpha_i} = \frac{1}{x}\frac{1}{1-\frac{\alpha_i}{x}} = \frac{1}{x}\sum_j(\frac{\alpha_i}{x})^j$ en la identidad anterior y agrupando en las potencias de $\frac{1}{x}$ se concluye.

(5) Resulta de igualar coeficientes en las potencias de x en la identidad $P'(x) = P(x)\cdot\sum_i \frac{\sigma_i}{x^{i+1}}$.

□

2.5. k-álgebras finitas.

1. Definición : Diremos que una k-álgebra A, es una k-álgebra finita, si A es un k-espacio vectorial de dimensión finita.

2. Ejemplo : Las extensiones finitas de cuerpos, de un cuerpo k, son k-álgebras finitas.

3. Ejemplo : $A = k[x]/(x^n + a_1x^{n-1} + \ldots + a_n)$ es una k-álgebra finita de base $\{1, \bar{x}, \ldots, \bar{x}^{n-1}\}$, por la proposición 2.1.2.

4. Proposición : *Toda k-álgebra finita e íntegra es cuerpo.*

Demostración. Sea A una k-álgebras finita íntegra. Dado $a \in A$ no nula, la homotecia $A \xrightarrow{\cdot a} A$, $b \mapsto b\cdot a$ es inyectiva, por ser A íntegra. Por tanto, por dimensiones, es isomorfismo. Luego a es invertible y A es cuerpo. □

5. Proposición : *El espectro primo de una k-álgebra finita A es un número finito ideales maximales. Además,*

$$\#\operatorname{Spec} A \leq \dim_k A$$

Demostración. Si hacemos cociente por un ideal primo obtenemos una k-álgebra finita íntegra, luego es un cuerpo por la proposición anterior. Por tanto, todos los ideales primos son maximales.

Sean $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$ ideales maximales distintos de A. Las inclusiones

$$A \supset \mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$$

son estrictas, porque $(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r)_0 = \cup_j(\mathfrak{m}_j)_0 = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$, luego $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r \neq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r \cap \mathfrak{m}_{r+1}$. Los ideales $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$ son en particular k-espacios vectoriales y $\dim_k(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r) > \dim_k(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{r+1})$. Por tanto, $\dim_k A \geq n$. Luego, $\#\operatorname{Spec} A \leq \dim_k A$.

□

6. Definición : Se dice que un anillo es local cuando sólo contiene un único ideal maximal.

7. Proposición : *Toda k-álgebra finita es un producto cartesiano de un número finito de k-álgebras finitas locales.*

Demostración. Sean $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$ los ideales maximales de A (que es el conjunto de todos los ideales primos de A). Sabemos que $\operatorname{rad} A = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. Escribamos $(a_1, \ldots, a_r) := \mathfrak{m}_1 \cdots \mathfrak{m}_n \subseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n = \operatorname{rad} A$. Existe s tal que $a_i^s = 0$, para todo i. Sea $N = r\cdot s$, entonces $(a_1, \ldots, a_r)^N = 0$. En conclusión, $\mathfrak{m}_1^N \cdots \mathfrak{m}_n^N = (\mathfrak{m}_1 \cdots \mathfrak{m}_n)^N = 0$.

Observemos que $\mathfrak{m}_1^N + (\mathfrak{m}_2^N \cdots \mathfrak{m}_n^N) = A$, porque

$$(\mathfrak{m}_1^N + (\mathfrak{m}_2^N \cdots \mathfrak{m}_n^N))_0 = (\mathfrak{m}_1^N)_0 \cap (\mathfrak{m}_2^N \cdots \mathfrak{m}_n^N))_0 = \{\mathfrak{m}_1\} \cap \{\mathfrak{m}_2, \ldots, \mathfrak{m}_n\} = \emptyset$$

Por el teorema chino de los restos

$$A = A/\mathfrak{m}_1^N \cdots \mathfrak{m}_n^N = A/\mathfrak{m}_1^N \times A/\mathfrak{m}_2^N \cdots \mathfrak{m}_n^N$$

Igualmente, $\mathfrak{m}_2^N + (\mathfrak{m}_3^N \cdots \mathfrak{m}_n^N) = A$, luego

$$A/\mathfrak{m}_2^N \cdots \mathfrak{m}_n^N = A/\mathfrak{m}_2^N \times A/\mathfrak{m}_3^N \cdots \mathfrak{m}_n^N$$

Repitiendo sucesivamente este último argumento, obtenemos

$$A = A/\mathfrak{m}_1^N \times \cdots \times A/\mathfrak{m}_n^N$$

Por último, $\operatorname{Spec}(A/\mathfrak{m}_i^N) = (\mathfrak{m}_i^N)_0 = (\mathfrak{m}_i)_0 = \{\mathfrak{m}_i\}$, luego $A/\mathfrak{m}_i^N$ es local. □

2.6. Teorema de Kronecker para k-álgebras finitas

1. Definición : Dada una k-álgebra A, decimos que $x \in \operatorname{Spec} A$ es un punto racional si $A/\mathfrak{p}_x = k$.

2. Definición : Sea A una k-álgebra finita. Diremos que A es racional si todos los puntos de su espectro son racionales. Diremos que una extensión de cuerpos $k \hookrightarrow K$ racionaliza a una k-álgebra A si $A \otimes_k K$ es una K-álgebra racional.

3. Ejemplo : Dada $\alpha \in k$, entonces $k[x]/((x-\alpha)^n)$ es una k-álgebra racional.

Dado un punto racional $x \in \operatorname{Spec} A$ tenemos el morfismo de paso al cociente $A \to A/\mathfrak{p}_x = k$. Recíprocamente, dado un morfismo $\phi\colon A \to k$, entonces $\mathfrak{p}_x = \operatorname{Ker}\phi$ es un punto racional. En conclusión,

$$\operatorname{Hom}_{k-alg}(A,k) = \{\text{Puntos racionales de } A\} \subseteq \operatorname{Spec} A$$

4. Proposición : *Una k-álgebra finita A es racional si y sólo si* $\#\operatorname{Hom}_{k-alg}(A,k) = \#\operatorname{Spec} A$.

5. Fórmula de los puntos : *Sea A una k-álgebra y $k \to K$ una extensión de cuerpos. Entonces*

$$\operatorname{Hom}_{k-alg}(A,K) = \operatorname{Hom}_{K-alg}(A \otimes_k K, K) = \{\textit{Puntos } K\textit{-racionales de } A \otimes_k K\}$$

En particular, $\#\operatorname{Hom}_{k-alg}(A,K) \leq \#\operatorname{Spec}(A \otimes_k K) \leq \dim_K(A \otimes_k K) = \dim_k A$.

Demostración. Es consecuencia de 1.4.5. □

6. Definición : Diremos que $\operatorname{Hom}_{k-alg}(A,K)$ son los puntos de A con valores en K.

Si $A = k[x]/(p(x))$, entonces los puntos de A con valores en K se corresponden biyectivamente con las raíces de $p(x)$ en K.

7. Ejercicio : Sea $A = k[x]/(p(x))$. Probar que A es racional si y sólo si $p(x)$ descompone en producto de factores simples $(x-\alpha_i)$ (repetidos o no). Probar que $A \otimes_k K$ es una K-álgebra racional si y sólo si K contiene todas las raíces de $p(x)$.

8. Proposición : *Si A es una k-álgebra finita local racional y $k \hookrightarrow K$ es una extensión finita de cuerpos, entonces $A \otimes_k K$ es una K-álgebra finita local K-racional.*

Demostración. Si $\mathfrak{p} \subset A$ es un ideal primo tal que $A/\mathfrak{p} = k$, entonces el ideal $\mathfrak{p} \otimes_k K \subset A \otimes_k K$ cumple que

$$(A \otimes_k K)/(\mathfrak{p} \otimes_k K) = (A/\mathfrak{p}) \otimes_k K = k \otimes_k K = K$$

Por ser $\mathfrak{p} \subset A$ el único ideal primo de A sus elementos son nilpotentes. Por tanto, los elementos de $\mathfrak{p} \otimes_k K \subset A \otimes_k K$ son nilpotentes. Luego, $\operatorname{Spec}(A \otimes_k K) = (\mathfrak{p} \otimes_k K)_0 = \{\mathfrak{p} \otimes_k K\}$. En conclusión, $A \otimes_k K$ es una K-álgebra finita local K-racional.

□

9. Teorema (Kronecker): *Si $k \hookrightarrow A$ es una k-álgebra finita, existe una extensión finita de cuerpos $k \hookrightarrow K$, de modo que $A \otimes_k K$ es una K-álgebra finita racional.*

Demostración. Procedemos por inducción sobre la dimensión de A, siendo el caso de dimensión uno inmediato. Sea K un cuerpo residual de A, que es una extensión finita de k. Por la fórmula de los puntos, el morfismo de paso al cociente $A \to K$ se corresponde con un punto K-racional de A_K. Por el teorema de descomposición se tiene que A_K descompone

$$A_K = A' \times A''$$

con A' una K-álgebra finita local y racional. Ahora,

$$\dim_K A'' < \dim_K A_K = \dim_k A$$

luego por inducción existe una extensión finita $K \to \Sigma$ tal que $A'' \otimes_K \Sigma$ es Σ-racional. Entonces $A \otimes_k \Sigma$ es Σ-álgebra finita Σ-racional; en efecto:

$$A \otimes_k \Sigma = (A \otimes_k K) \otimes_K \Sigma = (A' \times A'') \otimes_K \Sigma = (A' \otimes_K \Sigma) \times (A'' \otimes_K \Sigma)$$

que es una Σ-álgebra racional. □

2.7. Biografía de Kronecker

KRONECKER BIOGRAPHY

Leopold Kronecker's parents were well off, his father, Isidor Kronecker, being a successful business man while his mother was Johanna Prausnitzer who also came from a wealthy family. The families were Jewish, the religion that Kronecker kept until a year before his death when he became a convert to Christianity. Kronecker's parents employed private tutors to teach him up to the stage when he entered the Gymnasium at Liegnitz, and this tutoring gave him a very sound foundation to his education.

Kronecker was taught mathematics at Liegnitz Gymnasium by Kummer, and it was due to Kummer that Kronecker became interested in mathematics. Kummer immediately recognised Kronecker's talent for mathematics and he took him well beyond what would be expected at school, encouraging him to undertake research. Despite his Jewish upbringing, Kronecker was given Evangelical religious instruction at the Gymnasium which certainly shows that his parents were openminded on religious matters.

Kronecker became a student at Berlin University in 1841 and there he studied under Dirichlet and Steiner. He did not restrict himself to studying mathematics, however, for he studied other topics such as astronomy, meteorology and chemistry. He was especially interested in philosophy studying the philosophical works of Descartes, Leibniz, Kant, Spinoza and Hegel. After spending the summer of 1843 at the University of Bonn, which he went to because of his interest in astronomy rather than mathematics, he then went to the University of Breslau for the winter semester of 1843-44. The reason that he went to Breslau was certainly because of his interest in mathematics because he wanted to study again with his old school teacher Kummer who had been appointed to a chair at Breslau in 1842.

Kronecker spent a year at Breslau before returning to Berlin for the winter semester of 1844-45. Back in Berlin he worked on his doctoral thesis on algebraic number theory under Dirichlet's supervision. The thesis,

On complex units was submitted on 30 July 1845 and he took the necessary oral examination on 14 August. Dirichlet commented on the thesis saying that in it Kronecker showed:

... unusual penetration, great assiduity, and an exact knowledge of the present state of higher mathematics.

It may come as a surprise to many Ph.D. students to hear that Kronecker was questioned at his oral on a wide range of topics including the theory of probability as applied to astronomical observations, the theory of definite integrals, series and differential equations, as well as on Greek, and the history of philosophy.

Jacobi had health problems which caused him to leave Königsberg, where he held a chair, and return to Berlin. Eisenstein, whose health was also poor, lectured in Berlin around this time and Kronecker came to know both men well. The direction that Kronecker's mathematical interests went later had much to do with the influence of Jacobi and Eisenstein around this time. However, just as it looked as if he would embark on an academic career, Kronecker left Berlin to deal with family affairs. He helped to manage the banking business of his mother's brother and, in 1848, he married the daughter of this uncle, Fanny Prausnitzer. He also managed a family estate but still found the time to continue working on mathematics, although he did this entirely for his own enjoyment.

Certainly Kronecker did not need to take on paid employment since he was by now a wealthy man. His enjoyment of mathematics meant, however, that when circumstances changed in 1855 and he no longer needed to live on the estate outside Liegnitz, he returned to Berlin. He did not wish a university post, rather he wanted to take part in the mathematical life of the university and undertake research interacting with the other mathematicians.

In 1855 Kummer came to Berlin to fill the vacancy which occurred when Dirichlet left for Göttingen. Borchardt had lectured at Berlin since 1848 and, in late 1855, he took over the editorship of Crelle's Journal on Crelle's death. In 1856 Weierstrass came to Berlin, so within a year of Kronecker returning to Berlin, the remarkable team of Kummer, Borchardt, Weierstrass and Kronecker was in place in Berlin.

Of course since Kronecker did not hold a university appointment, he did not lecture at this time but was remarkably active in research publishing a large number of works in quick succession. These were on number theory, elliptic functions and algebra, but, more importantly, he explored the interconnections between these topics. Kummer proposed Kronecker for election to the Berlin Academy in 1860, and the proposal was seconded by Borchardt and Weierstrass. On 23 January 1861 Kronecker was elected to the Academy and this had a surprising benefit.

Members of the Berlin Academy had a right to lecture at Berlin University. Although Kronecker was not employed by the University, or any other organisation for that matter, Kummer suggested that Kronecker exercise his right to lecture at the University and this he did beginning in October 1862. The topics on which he lectured were very much related to his research: number theory, the theory of equations, the theory of determinants, and the theory of integrals. In his lectures [1]:

He attempted to simplify and refine existing theories and to present them from new perspectives.

For the best students his lectures were demanding but stimulating. However, he was not a popular teacher with the average students [1]:

Kronecker did not attract great numbers of students. Only a few of his auditors were able to follow the flights of his thought, and only a few persevered until the end of the semester.

Berlin was attractive to Kronecker, so much so that when he was offered the chair of mathematics in Göttingen in 1868, he declined. He did accept honours such as election to the Paris Academy in that year and for many years he enjoyed good relations with his colleagues in Berlin and elsewhere. In order to understand why relations began to deteriorate in the 1870s we need to examine Kronecker's mathematical contributions more closely.

We have already indicated that Kronecker's primary contributions were in the theory of equations and higher algebra, with his major contributions in elliptic functions, the theory of algebraic equations, and the

theory of algebraic numbers. However the topics he studied were restricted by the fact that he believed in the reduction of all mathematics to arguments involving only the integers and a finite number of steps. Kronecker is well known for his remark:

God created the integers, all else is the work of man.

Kronecker believed that mathematics should deal only with finite numbers and with a finite number of operations. He was the first to doubt the significance of non-constructive existence proofs. It appears that, from the early 1870s, Kronecker was opposed to the use of irrational numbers, upper and lower limits, and the Bolzano-Weierstrass theorem, because of their non-constructive nature. Another consequence of his philosophy of mathematics was that to Kronecker transcendental numbers could not exist.

In 1870 Heine published a paper On trigonometric series in Crelle's Journal, but Kronecker had tried to persuade Heine to withdraw the paper. Again in 1877 Kronecker tried to prevent publication of Cantor's work in Crelle's Journal, not because of any personal feelings against Cantor (which has been suggested by some biographers of Cantor) but rather because Kronecker believed that Cantor's paper was meaningless, since it proved results about mathematical objects which Kronecker believed did not exist. Kronecker was on the editorial staff of Crelle's Journal which is why he had a particularly strong influence on what was published in that journal. After Borchardt died in 1880, Kronecker took over control of Crelle's Journal as the editor and his influence on which papers would be published increased.

The mathematical seminar in Berlin had been jointly founded in 1861 by Kummer and Weierstrass and, when Kummer retired in 1883, Kronecker became a codirector of the seminar. This increased Kronecker's influence in Berlin. Kronecker's international fame also spread, and he was honoured by being elected a foreign member of the Royal Society of London on 31 January 1884. He was also a very influential figure within German mathematics [1]:

He established other contacts with foreign scientists in numerous travels abroad and in extending to them the hospitality of his Berlin home. For this reason his advice was often solicited in regard to filling mathematical professorships both in Germany and elsewhere; his recommendations were probably as significant as those of his erstwhile friend Weierstrass.

Although Kronecker's view of mathematics was well known to his colleagues throughout the 1870s and 1880s, it was not until 1886 that he made these views public. In that year he argued against the theory of irrational numbers used by Dedekind, Cantor and Heine giving the arguments by which he opposed:

... the introduction of various concepts by the help of which it has frequently been attempted in recent times (but first by Heine) to conceive and establish the "irrationals"in general. Even the concept of an infinite series, for example one which increases according to definite powers of variables, is in my opinion only permissible with the reservation that in every special case, on the basis of the arithmetic laws of constructing terms (or coefficients), ... certain assumptions must be shown to hold which are applicable to the series like finite expressions, and which thus make the extension beyond the concept of a finite series really unnecessary.

Lindemann had proved that π is transcendental in 1882, and in a lecture given in 1886 Kronecker complimented Lindemann on a beautiful proof but, he claimed, one that proved nothing since transcendental numbers did not exist. So Kronecker was consistent in his arguments and his beliefs, but many mathematicians, proud of their hard earned results, felt that Kronecker was attempting to change the course of mathematics and write their line of research out of future developments. Kronecker explained his programme based on studying only mathematical objects which could be constructed with a finite number of operation from the integers in Über den Zahlbergriff in 1887.

Another feature of Kronecker's personality was that he tended to fall out personally with those who he disagreed with mathematically. Of course, given his belief that only finitely constructible mathematical objects existed, he was completely opposed to Cantor's developing ideas in set theory. Not only Dedekind, Heine and Cantor's mathematics was unacceptable to this way of thinking, and Weierstrass also came to feel that

Kronecker was trying to convince the next generation of mathematicians that Weierstrass's work on analysis was of no value.

Kronecker had no official position at Berlin until Kummer retired in 1883 when he was appointed to the chair. But by 1888 Weierstrass felt that he could no longer work with Kronecker in Berlin and decided to go to Switzerland, but then, realising that Kronecker would be in a strong position to influence the choice of his successor, he decided to remain in Berlin.

Kronecker was of very small stature and extremely self-conscious about his height. An example of how Kronecker reacted occurred in 1885 when Schwarz sent him a greeting which included the sentence:

He who does not honour the Smaller, is not worthy of the Greater.

Here Schwarz was joking about the small man Kronecker and the large man Weierstrass. Kronecker did not see the funny side of the comment, however, and never had any further dealings with Schwarz (who was Weierstrass's student and Kummer's son-in-law). Others however displayed more tact and, for example, Helmholtz who was a professor in Berlin from 1871, managed to stay on good terms with Kronecker.

The Deutsche Mathematiker-Vereinigung was set up in 1890 and the first meeting of the Association was organised in Halle in September 1891. Despite the bitter antagonism between Cantor and Kronecker, Cantor invited Kronecker to address this first meeting as a sign of respect for one of the senior and most eminent figures in German mathematics. However, Kronecker never addressed the meeting, since his wife was seriously injured in a climbing accident in the summer and died on 23 August 1891. Kronecker only outlived his wife by a few months, and died in December 1891.

We should not think that Kronecker's views of mathematics were totally eccentric. Although it was true that most mathematicians of his day would not agree with those views, and indeed most mathematicians today would not agree with them, they were not put aside. Kronecker's ideas were further developed by Poincaré and Brouwer, who placed particular emphasis upon intuition. Intuitionism stresses that mathematics has priority over logic, the objects of mathematics are constructed and operated upon in the mind by the mathematician, and it is impossible to define the properties of mathematical objects simply by establishing a number of axioms.

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/)

2.8. Problemas

1. Sea $A = \mathbb{Q}[x]/(2x^3 + 4x^2 - x - 2)$ y sea $\alpha = \bar{x}$. ¿Son $\alpha + 2$ y $\alpha - 2$ invertibles en A?.

2. Sea $K = \mathbb{Q}[x]/(x^3 - x - 1)$ y sea $\alpha = \bar{x}$. Racionalizar $1/(\alpha + 2)$ y determinar si $(2 + \alpha)^3$ es la unidad. ¿Tiene el polinomio $x^2 - 2$ alguna raíz en K?. Calcular un polinomio no nulo con coeficientes racionales $p(x)$ que admita la raíz $\beta = \alpha^2 + 1$.

3. Si $a, b \in \mathbb{Q}$, demostrar que $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ precisamente cuando a/b sea un cuadrado en $\mathbb{Q}$.

4. Demostrar que $\mathbb{Q}(\sqrt[3]{2})$ es una extensión de grado 3 de $\mathbb{Q}$. ¿Está $\sqrt{2}$ en $\mathbb{Q}(\sqrt[3]{2})$?
   Demostrar que $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. ¿Está $\sqrt[3]{2}$ en $\mathbb{Q}(\sqrt[4]{2})$?

5. Determinar si las siguientes igualdades son ciertas:

$$\begin{aligned} \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) &= \mathbb{Q}(\sqrt[4]{2}, i) \\ \mathbb{Q}(2^{-1/2}, i) &= \mathbb{Q}(i\sqrt{2}) \\ \mathbb{Q}(2^{-1/2}, i) &= \mathbb{Q}(i + \sqrt{2}) \end{aligned}$$

6. Determinar las relaciones de inclusión entre los siguientes subcuerpos de $\mathbb{C}$:
$$\mathbb{Q}\ ,\ \mathbb{Q}(1/2)\ ,\ \mathbb{Q}(\sqrt{2}\,)\ ,\ \mathbb{Q}(\sqrt[3]{2}\,)\ ,\ \mathbb{Q}(i)\ ,\ \mathbb{Q}(i+\sqrt{2}\,)\ ,\ \mathbb{Q}(\sqrt{-2}\,)$$

7. Sea $p(x)$ un polinomio irreducible de grado n con coeficientes en un cuerpo k. Si el grado de una extensión finita L de k no es múltiplo de n, entonces $p(x)$ no tiene raíces en L.

8. Demostrar que $x^3 - 3$ no tiene raíces en $k = \mathbb{Q}(\sqrt{2})$. Concluir que $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}\,)$ es una extensión de grado 6 de $\mathbb{Q}$ y hallar una base sobre $\mathbb{Q}$.

   Sea $\alpha = \sqrt{2} + \sqrt[3]{3}$. Probar que el grado de un polinomio irreducible en $\mathbb{Q}[x]$ que admita la raíz α es $[\mathbb{Q}(\alpha)\colon \mathbb{Q}] = 1, 2, 3,$ ó 6. Analizando las relaciones de dependencia lineal entre las sucesivas potencias de α, concluir que α es raíz de un polinomio irreducible de grado 6 con coeficientes racionales. Calcular tal polinomio.

9. Sea $K = \mathbb{F}_2[x]/(x^3 + x + 1)$ y sea $\alpha = \bar{x}$. Probar que K es un cuerpo con 8 elementos
$$K = \{0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7 = 1\}$$
   Calcular las raíces de $x^3 + x + 1$ en K, y las raíces de $x^3 + x^2 + 1$ en K.

10. Construir un cuerpo con 4 elementos y otro con 9 elementos.

11. Calcular el grado (y una base) sobre $\mathbb{Q}$ de la extensión que generan las raíces complejas del polinomio $x^3 - 1$. Análogamente para $x^3 + 1$, $x^4 - 1$, $x^4 + 1$, $x^5 - 1$, $x^5 + 1$ y $x^6 - 1$.

12. Hallar el grado (y una base) sobre $\mathbb{Q}$ de la extensión que generan todas las raíces complejas del polinomio $x^3 - 2$. Análogamente para los polinomios
$$x^4 - 2\ ,\ x^4 + 2\ ,\ x^4 - x^2 + 1\ ,\ x^4 + x^2 - 2,\ x^3 - 4x^2 + 5$$

13. Probar que $\mathbb{Q}(\sqrt[n]{2}\,)$ tiene grado n sobre $\mathbb{Q}$.

14. Calcular un polinomio irreducible con coeficientes en $\mathbb{Q}(i)$ que admita la raíz $\sqrt[4]{2}$.

    Análogamente sustituyendo $\mathbb{Q}(i)$ por $\mathbb{Q}(\sqrt{2}\,)$ y $\mathbb{Q}(\sqrt[3]{2}\,)$.

15. Determinar si $\sqrt{2} + \sqrt[3]{3}$, $\sqrt[4]{2}$ y $\sqrt[5]{2}$ son irracionales cuadráticos.

16. Sea K una extensión de grado 2 de un cuerpo k. Si la característica de k no es 2, probar que $K = k(\sqrt{a}$ para algún $a \in k$. ¿Es cierto también cuando $\operatorname{car} k = 2$?

17. Hallar un polinomio $p(x) \in \mathbb{Q}[x]$ tal que $\mathbb{Q}(i) \oplus \mathbb{Q}(\sqrt[3]{2}\,) \simeq \mathbb{Q}[x]/(p(x))$.

18. ¿Existe algún polinomio $p(x) \in \mathbb{Q}[x]$ tal que $\mathbb{Q}(i) \oplus \mathbb{Q}(i) \simeq \mathbb{Q}[x]/(p(x))$?

19. Sean $\alpha_1, \ldots, \alpha_n$ raíces complejas de ciertos polinomios no nulos $p_1(x), \ldots, p_n(x) \in \mathbb{Q}[x]$. Demostrar que $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ es una $\mathbb{Q}$-álgebra finita de grado acotado por el producto de los grados de los polinomios $p_1(x), \ldots, p_n(x)$.

20. Una extensión finita $k \to L$ es trivial (i.e., $[L : k] = 1$) si y sólo si $L \otimes_k L$ es cuerpo.

    (*Indicación:* Considerar el morfismo natural $L \otimes_k L \to L$).

21. Si L y L' son dos extensiones no triviales (i.e., de grado mayor que 1) de un cuerpo k, ¿puede ocurrir que $L' \otimes_k L$ no sea un cuerpo? ¿y que $L' \otimes_k L$ sí sea un cuerpo?.

22. Probar que toda extensión finita L de $\mathbb{C}$ es trivial: $\mathbb{C} \simeq L$. Concluir que toda $\mathbb{C}$–álgebra finita reducida de grado n es isomorfa a $\mathbb{C} \oplus \overset{n}{\cdots} \oplus \mathbb{C}$. ¿Es cierto que toda $\mathbb{C}$–álgebra finita es trivial?

23. Probar que toda extensión finita de $\mathbb{R}$ es isomorfa a $\mathbb{R}$ ó a $\mathbb{C}$. Concluir que toda $\mathbb{R}$–álgebra finita reducida es isomorfa a $\mathbb{R} \oplus \overset{n}{\cdots} \oplus \mathbb{R} \oplus \mathbb{C} \oplus \overset{m}{\cdots} \oplus \mathbb{C}$ para ciertos $n, m \in \mathbb{N}$.

24. Sean L y L' dos extensiones finitas de un cuerpo k. Si sus respectivos grados son primos entre sí, probar que $L \otimes_k L'$ es cuerpo.

25. Determinar los automorfismos de los cuerpos $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt[5]{2})$ y $\mathbb{Q}(\sqrt[6]{2})$.

26. Determinar los automorfismos de la extensión de $\mathbb{Q}$ que generan todas las raíces complejas de $x^3 - 3$. Análogamente para $x^2 - 2$, $x^4 - 4$.

27. Sea $k = \mathbb{Q}(\sqrt[5]{5})$. Probar que el polinomio irreducible de $e^{\frac{2\pi i}{5}}$ sobre k es $x^4 + x^3 + x^2 + x + 1$.

    Determinar el número de automorfismos de la extensión de $\mathbb{Q}$ que generan todas las raíces complejas de $x^5 - 5$.

28. Sea $p(x)$ un polinomio no constante con coeficientes en un cuerpo k. Probar que α es una raíz múltiple de $p(x)$ si y sólo si es raíz de $p(x)$ y $p'(x)$. Probar que si α es una raíz de $p(x)$ de multiplicidad $m \geq 2$, entonces α es una raíz de $p'(x)$ de multiplicidad $m - 1$, cuando la característica de k es cero. Probar que si α es una raíz de $p(x)$ de multiplicidad $m \geq 2$, entonces α es una raíz de $p'(x)$ de multiplicidad mayor o igual que $m - 1$, cuando la característica de k es positiva.

29. Sea $p(x)$ un polinomio no constante con coeficientes en un cuerpo k, de característica nula. Probar que si m es la multiplicidad de una raíz α del polinomio $d(x) = \text{m.c.d.}(p(x), p'(x))$, entonces α es una raíz de $p(x)$ de multiplicidad $m + 1$.

    ¿Es cierto este enunciado en los cuerpos de característica positiva?

30. Sea $p(x)$ un polinomio irreducible con coeficientes en un cuerpo. Probar que si $p(x)$ tiene alguna raíz múltiple, entonces su derivada $p'(x)$ es nula.

    Si $p(x)$ tiene una raíz simple ¿es cierto que todas sus raíces son simples?. Si $p(x)$ tiene una raíz múltiple ¿es cierto que todas sus raíces son múltiples?

31. Hallar las raíces múltiples de los siguientes polinomios con coeficientes racionales, así como sus respectivas multiplicidades ¿y si los coeficientes están en $\mathbb{F}_2$? ¿y en $\mathbb{F}_3$? ¿y en $\mathbb{F}_5$?

$$x^4 + 4x^2 + 1 \quad , \quad 4x^4 - 4x^3 - 3x^2 + 2x + 1$$

Capítulo 3

Teoría de Galois

3.1. Introducción

Dado un polinomio $p(x) \in k[x]$, consideremos una extensión de cuerpos $k \hookrightarrow L$, de modo que $p(x) = a_0 \cdot (x - \alpha_1) \cdots (x - \alpha_n)$, con $\alpha_1, \ldots, \alpha_n \in L$.

¿Pueden obtenerse las raíces $\alpha_1, \ldots, \alpha_n$ de $p(x)$ mediante expresiones algebraicas de radicales de elementos de k?

Sea $k(\alpha_1, \ldots, \alpha_n) \subseteq L$ el mínimo subcuerpo de L que contiene a $\alpha_1, \ldots, \alpha_n$ (y k), que se denomina el cuerpo de descomposición de $p(x)$. Consideremos el epimorfismo

$$k[x_1, \ldots, x_n] \xrightarrow{\phi} k(\alpha_1, \ldots, \alpha_n) \subset L, \quad \phi(q(x_1, \ldots, x_n)) := q(\alpha_1, \ldots, \alpha_n)$$

Entonces, $k(\alpha_1, \ldots, \alpha_n) = k[x_1, \ldots, x_n]/I$, con $I = \{q(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] \colon q(\alpha_1, \ldots, \alpha_n) = 0\}$. Los automorfismos de k-álgebras de $k(\alpha_1, \ldots, \alpha_n)$, han de permutar las raíces de $p(x)$, es más, están en correspondencia biunívoca con las permutaciones de las raíces tales que si unas cuantas raíces verifican una relación algebraica entonces sus permutadas verifican la misma relación. La teoría de Galois clásica demuestra que el grupo (de Galois) de los automorfismos del cuerpo de descomposición de $p(x)$ es resoluble si y sólo si las raíces de $p(x)$ se pueden obtener mediante radicales, y en el caso resoluble da el procedimiento para obtener las raíces.

Tanto $k[x]/(p(x))$ como $k(\alpha_1, \ldots, \alpha_n)$ son k-álgebras finitas. En el estudio de las variedades algebraicas es obligado comenzar con las variedades algebraicas de dimensión cero, es decir, con el estudio (del espectro primo) de las k-álgebras finitas. Puede decirse que la Teoría de Galois estudia y clasifica las variedades algebraicas de dimensión cero.

3.2. k-álgebras finitas triviales y separables

1. Definición : Diremos que una k-álgebra finita A es trivial si existe un isomorfismo de k-álgebras $A \simeq k \times \ldots \times k$.

2. Ejemplo : Sea $p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, con $\alpha_i \neq \alpha_j \in k$ cuando $i \neq j$. Por el teorema chino de los restos

$$k[x]/(p(x)) = k[x]/(x - \alpha_1) \times \overset{n}{\cdots} \times k[x]/(x - \alpha_n) = k \times \overset{n}{\cdots} \times k$$

es una k-álgebra trivial.

3. Ejemplo : Sea $X = \{x_1, \ldots, x_n\}$ un conjunto finito y $A = \mathrm{Aplic}(X, k)$, que es un anillo con la suma y producto usual de funciones. A es una k-álgebra finita trivial de grado n, pues el morfismo

$$\mathrm{Aplic}(X, k) \to k \times \overset{n}{\cdots} \times k, \;\; f \mapsto (f(x_1), \ldots, f(x_n))$$

es un isomorfismo de k-álgebras.

Obviamente, las k-álgebras finitas triviales son racionales. Por tanto,

$$\mathrm{Hom}_{k-alg}(k^n, k) \overset{2.6.4}{=} \mathrm{Spec}\, k^n, \;\; \phi \mapsto \mathrm{Ker}\, \phi$$

que es un conjunto de orden n. Explícitamente, los morfismos de k-álgebras de k^n en k son las n-proyecciones distintas, $(\lambda_1, \cdots, \lambda_n) \mapsto \lambda_i$.

4. Proposición: *Sea A una k-álgebra finita. Entonces,*

1. *A es una k-álgebra finita trivial si y sólo si $\#\,\mathrm{Spec}\, A = \dim_k A$.*
2. *A es una k-álgebra finita trivial si y sólo si $\#\,\mathrm{Hom}_{k-alg}(A, k) = \dim_k A$.*

Demostración. 1. Si $\mathrm{Spec}\, A = \{x_1, \ldots, x_n\}$, entonces por 2.5.7, A es producto cartesiano de n k-álgebras finitas locales

$$A = A_1 \times \ldots \times A_n$$

Por tanto, $\#\,\mathrm{Spec}\, A = \dim_k A$ si y sólo si $\dim_k A_i = 1$, para todo i, es decir, si y sólo si A es trivial.

2. En general sabemos que $\#\,\mathrm{Hom}_{k-alg}(A, k) \leq \#Spec A \leq \dim_k A$. Si $\#\,\mathrm{Hom}_{k-alg}(A, k) = \dim_k A$, entonces $\#Spec A = \dim_k A$ y A es trivial. Si $A = k^n$ es trivial, entonces tenemos n proyecciones de A en k obvias, luego $\mathrm{Hom}_{k-alg}(A, k) \geq n = \dim_k A$ y $\#\,\mathrm{Hom}_{k-alg}(A, k) = \dim_k A$.

□

5. Ejercicio : Probar:

1. Si A es una k-álgebra finita trivial, entonces A_K es una K-álgebra trivial, para toda extensión $k \to K$.
2. El producto tensorial de dos k-álgebras finitas triviales es una k-álgebra finita trivial.
3. Las subálgebras y las k-álgebras cocientes de una k-álgebra finita trivial son triviales.

6. Definición : Se dice que una k-álgebra finita A es separable si existe una extensión cuerpos $k \hookrightarrow K$ tal que $A \otimes_k K = \prod_i K$. También se dice que A es separable sobre k.

Las k-álgebras finitas triviales son k-álgebras finitas separables.

7. Ejercicio : La k-álgebra $k[x]/(p(x))$ es separable si y sólo si $p(x)$ y $p'(x)$ son primos entre sí, es decir, $p(x)$ no tiene raíces múltiples.

8. Proposición: *Sea A una k-álgebra finita y $k \to K$ una extensión de cuerpos. Entonces, A es separable sobre k si y sólo si A_K es separable sobre K.*

Demostración. Si Σ trivializa a A cualquier extensión, Σ', de Σ también, porque $A \otimes_k \Sigma' = (A \otimes_k \Sigma) \otimes_\Sigma \Sigma'$.

Si A es separable, sea Σ una extensión trivializante de A y Σ' un compuesto de K y Σ, entonces $(A \otimes_k K) \otimes_K \Sigma' = A \otimes_k \Sigma'$ es Σ'-trivial y $A \otimes_k K$ es K-separable.

Si A_K es K-separable, sea Σ una K-extensión trivializante de A_K. Entonces, $A \otimes_k \Sigma = A_K \otimes_K \Sigma$ es Σ-trivial y A es k-separable.

□

9. Ejercicio : Probar:

- $A \times B$ es separable si y sólo si A y B lo son.

- El producto tensorial (sobre k) de álgebras separables (sobre k) es separable (sobre k).

- Toda subálgebra y cociente de una k-álgebra separable es separable.

10. Proposición: *Una k-álgebra finita es separable si y sólo si A_K es reducida, para toda extensión de cuerpos, $k \to K$.*

Demostración. Sea A separable sobre k y $k \to K'$ una extensión cualquiera. Veamos que $A \otimes_k K'$ es reducida. Sea $k \to K$ una extensión que trivializa a A y K'' un compuesto de K y K'. Entonces

$$(A \otimes_k K') \otimes_{K'} K'' = A \otimes_k K'' = (A \otimes_k K) \otimes_K K'' = \prod \prod K''$$

Ahora bien, $A \otimes_k K'$ es una subálgebra de $\prod K''$, luego es reducida.

Recíprocamente, si A es reducida por todo cambio de base, considerando un cambio de base $k \to K$ racionalizante, se obtiene que A_K es racional y reducida, luego trivial. □

11. Proposición: *Una extensión de cuerpos $k \hookrightarrow K$ trivializa a una k-álgebra finita A si y sólo si*

$$\#\operatorname{Hom}_{k-alg}(A, K) = \dim_k A$$

Demostración. Por la fórmula de los puntos, $\operatorname{Hom}_{k-alg}(A, K)$ son los puntos K-racionales de $A \otimes_k K$. Ahora bien, $A \otimes_k K$ es una K-álgebra trivial si y sólo si el número de sus puntos K-racionales coincide con $\dim_K A_K$. Como $\dim_k A = \dim_K A_K$, se concluye. □

12. Proposición: *Sea k un cuerpo con infinitos elementos y A una k-álgebra finita separable. Existe un elemento $a \in A$ tal que $A = k[a]$. Dicho elemento se denomina elemento primitivo de A.*

Demostración. Sea $k \to K$ una extensión de cuerpos que trivialice a A. Si $\dim_k A = n$, entonces A tiene n puntos racionales. Escribamos $\{\phi_1, \ldots, \phi_n\} = \operatorname{Hom}_{k-\text{álg}}(A, K)$. Consideremos en A los hiperplanos $H_{ij} = \operatorname{Ker}(\phi_i - \phi_j)$, $i \neq j$. Sea $a \in A$ un elemento que no pertenezca a ninguno de dichos hiperplanos. Entonces, las restricciones de ϕ_i y ϕ_j a $k[a]$ son distintas, para todo $i \neq j$. Por tanto, $k[a]$ tiene al menos n puntos K-racionales, luego su dimensión es mayor o igual que n, luego $A = k[a]$. □

13. Definición : Sea A una k-álgebra finita. Se dice que un elemento $a \in A$ es separable (sobre k) si $k[a]$ es una k-álgebra separable (es decir, si el polinomio anulador mínimo de a no tiene raíces múltiples).

14. Proposición: *Una k-álgebra finita A, es separable si y sólo si todos sus elementos son separables.*

Demostración. Toda subálgebra de una k-álgebra separable es separable, luego todo elemento de una k-álgebra separable es separable.

Recíprocamente, veamos que si todo elemento es separable el álgebra es separable. Si $a_1, \ldots, a_r$ es una base, entonces A es un cociente de $k[a_1] \underset{k}{\otimes} \cdots \underset{k}{\otimes} k[a_n]$, luego es separable. □

Consideremos el morfismo de anillos

$$\varphi\colon \mathbb{Z} \to k,\ \varphi(n) = \begin{cases} 1 + \overset{n}{\ldots} + 1 & \text{si } n > 0 \\ -\varphi(-n) & \text{si } n < 0 \\ 0 & \text{si } n = 0 \end{cases}$$

15. Definición : Si $\operatorname{Ker}\varphi = 0$, se dice que k es un cuerpo de característica cero. En este caso, tendremos una inyección canónica $\mathbb{Q} \hookrightarrow k$. Si $\operatorname{Ker}\varphi \neq 0$, entonces $\operatorname{Ker}\varphi = (p)$, p primo. En este caso se dice que k es de característica p y tenemos una inyección canónica $\mathbb{Z}/p\mathbb{Z} \hookrightarrow k$.

16. Proposición : *Sea k un cuerpo de característica cero. Una k-álgebra finita A es separable si y sólo si es reducida.*

Demostración. Si A es separable es reducida por 3.2.10.

Si A es reducida entonces es producto directo de cuerpos. En característica cero las extensiones finitas de cuerpos son separables, porque todos sus elementos son separables: En efecto, el polinomio anulador $p(x)$ de un elemento es un polinomio irreducible, luego primo con su derivada $p'(x)$ (en característica cero $p'(x) \neq 0$), luego sin raíces múltiples.

□

3.3. Extensiones de Galois

1. Definición : Diremos que una extensión finita $k \to K$ es de *Galois* si se trivializa a si misma, esto es

$$K \underset{k}{\otimes} K \simeq K \times \cdots \times K$$

Se llama *grupo* de la extensión al grupo de automorfismos de K sobre k. En resumen, diremos que $k \to K$ *es una extensión de Galois de grupo G*, si es de Galois y $G = \operatorname{Aut}_{k-alg} K$.

Si $k \to K$ es de Galois, entonces $K \underset{k}{\otimes} K \simeq K \times \overset{n}{\cdots} \times K$, y $n = \dim_K(K \underset{k}{\otimes} K) = \dim_k K$ = grado de la extensión.

2. Proposición: *Una extensión $k \to K$ es de Galois si y sólo si el grado de la extensión coincide con el número de automorfismos,*

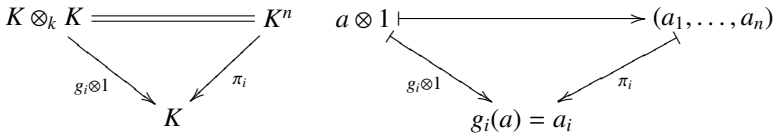
$$\dim_k K = \operatorname{Aut}_{k-alg} K$$

Demostración. Sabemos por la proposición 3.2.11, que K se trivializa a sí misma si y sólo tiene tantos endomorfismos (de k-álgebras) como grado. Como todo endomorfismo de k-álgebras de K es un automorfismo, se concluye. □

3. Observación : Sea $k \hookrightarrow K$ una extensión de Galois de grupo $G = \{g_1, \ldots, g_n\}$. Explicitemos el isomorfismo $K \otimes_k K = K \times \overset{n}{\cdots} \times K$. Tenemos,

$$\{g_1, \ldots, g_n\} = \operatorname{Hom}_{k-alg}(K, K) = \operatorname{Hom}_{K-alg}(K \otimes_k K, K) = \operatorname{Hom}_{K-alg}(K^n, K) = \{\pi_1, \ldots, \pi_n\}$$

donde π_i en la proyección en el factor i. De los diagramas conmutativos



se deduce, que el isomorfismo $K \otimes_k K = K^n$, asigna $a \otimes \lambda$ en $(g_1(a) \cdot \lambda, \ldots, g_n(a) \cdot \lambda)$.

4. Teorema: *Sea $k \hookrightarrow A$ una k-álgebra finita separable. Existe una extensión mínima de cuerpos que trivializa a A. Además, es única salvo isomorfismos y es Galois.*

Demostración. Sea $k \hookrightarrow K$ una extensión que trivialice a A. Tenemos que $\#\operatorname{Hom}_{k-alg}(A, K) = \#\operatorname{Spec}(A \otimes_k K) = n$. Sea $\{\phi_1, \ldots, \phi_n\} = \operatorname{Hom}_{k-alg}(A, K)$ y $\phi\colon A \otimes_k \overset{n}{\ldots} \otimes_k A \to K$, el morfismo de k-álgebras definido por $\phi(a_1 \otimes_k \ldots \otimes_k a_n) := \phi_1(a_1) \cdot \ldots \cdot \phi_n(a_n)$. $\Sigma = \operatorname{Im}\phi$, es una extensión que trivializa a A, porque $\#\operatorname{Hom}_{k-alg}(A, \Sigma) = n$. Σ es un cociente de $A \otimes_k \ldots \otimes_k A$, que está trivializado por Σ, luego Σ trivializa a Σ, es decir, es de Galois. De nuevo, si una extensión trivializa a A, trivializará a Σ, en particular, la contiene. De aquí se obtiene la unicidad y minimalidad de Σ. □

5. Definición: Si $k \hookrightarrow A$ es una k-álgebra finita separable, denominaremos envolvente de Galois de A sobre k, a la extensión mínima trivializante de A. Si $A = k[x]/(p(x))$, (con $p(x)$ sin raíces múltiple) la extensión mínima que trivializa a A, es el mínimo cuerpo que contiene a las raíces de $p(x)$. Cuerpo que denominaremos cuerpo de descomposición de $p(x)$, que es una extensión de Galois de k.

6. Observación: La envolvente de Galois está caracterizada por ser la única extensión (salvo isomorfismos) que trivializa a A y que es un cociente de un producto tensorial $A \otimes_k \cdots \otimes_k A$. En efecto, si $k \to \Omega$ es otra extensión que trivializa a A y que sea cociente de $A \otimes_k \cdots \otimes_k A$, entonces K trivializa a Ω (pues trivializa a A, luego a $A \otimes_k \cdots \otimes_k A$, luego a Ω por ser un cociente) y análogamente Ω trivializa a K. Por tanto, K contiene a Ω y viceversa, luego por dimensiones son isomorfos

7. Proposición: *Sea $k \to K$ una extensión finita separable. Las siguientes condiciones son equivalentes:*

1. *K es una extensión Galois de k.*
2. *Si $p(x) \in k[x]$ es un polinomio irreducible que tiene una raíz en K, entonces todas las raíces de $p(x)$ están en K. (Definición clásica de extensión de Galois).*
3. *("Agujero único en el cierre algebraico") Existe una única inmersión de K en el cierre algebraico de k, salvo automorfismos de K.*

Demostración. 1. $\Rightarrow$ 2.. Sea K una extensión de Galois de k, y sea $p(x) \in k[x]$ un polinomio irreducible que tiene una raíz en K. Dar una raíz equivale a dar un morfismo

$$k[x]/(p(x)) \to K$$

necesariamente inyectivo, pues $k[x]/(p(x))$ es cuerpo, ya que $p(x)$ es irreducible. Tensorializando por K obtenemos

$$K[x]/(p(x)) = k[x]/(p(x)) \underset{k}{\otimes} K \hookrightarrow K \underset{k}{\otimes} K$$

y como $K \underset{k}{\otimes} K$ es trivial, $K[x]/(p(x))$ también, es decir $p(x)$ tiene todas sus raíces en K.

2. $\Rightarrow$ 1. $K = k[\alpha_1, \ldots, \alpha_n]$ es cociente de un producto tensorial de álgebras del tipo $k[\alpha] = k[x]/(p(x))$, con $p(x)$ irreducible y sin raíces múltiples. $K \underset{k}{\otimes} k[\alpha] = K[x]/(p(x))$ y $\alpha \in K$ es una raíz de $p(x)$. Por la hipótesis, todas las raíces de $p(x)$ están en K, luego $K \underset{k}{\otimes} k[\alpha] = K[x]/(p(x))$ es trivial. Por tanto $K \otimes_k K$ es trivial, porque es cociente de un producto tensorial de álgebras triviales.

1. $\Leftrightarrow$ 3. El cierre algebraico de k, $\bar{k}$, trivializa a K. Luego, por 3.2.11, $\#Hom_{k-alg}(K, \bar{k}) = \dim_k K$. K es de Galois si y sólo K la trivializa. Por 3.2.11, K trivializa a K si y sólo si $\#\operatorname{Hom}_{k-alg}(K, K) = \dim_k K$. Por tanto, K trivializa a K si y sólo si $\operatorname{Hom}_{k-alg}(K, K) = \operatorname{Hom}_{k-alg}(K, \bar{k})$, es decir, si y sólo si existe una única inmersión de K en el cierre algebraico de k, salvo automorfismos de K.

□

8. Ejemplo: Si $k \hookrightarrow A$ es una k-álgebra separable, la extensión mínima trivializante de A es de Galois, pues es normal y es separable porque es un cociente de $A \otimes_k \cdots \otimes_k A$. Por ello la envolvente normal de un álgebra separable se denomina envolvente de Galois. Si $p(x) \in k[x]$ es un polinomio separable y $A = k[x]/(p(x))$, entonces la envolvente de Galois de A es $k(\alpha_1, \ldots, \alpha_n)$, siendo $\alpha_1, \ldots, \alpha_n$ las raíces de $p(x)$ (en el cierre algebraico de k).

9. Definición : Se llama *grupo de la ecuación* $p(x) = 0$, al grupo de automorfismos de su envolvente de Galois $k \to k(\alpha_1, \ldots, \alpha_n)$.

3.3.1. Extensiones ciclotómicas

Sea

$$\mu_n := \{\varepsilon_n^k = cos\,\frac{2k\pi}{n} + isen\,\frac{2k\pi}{n} \in \mathbb{C},\ 0 \le k < n\},$$

el conjunto de todas las raíces n-ésimas de la unidad, que es un subgrupo (multiplicativo) de $\mathbb{C}^*$, de orden n.

El morfismo, $\mathbb{Z}/n\mathbb{Z} \to \mu_n$, $\bar{m} \mapsto \varepsilon_n^m$ es un isomorfismo de grupos. Vía este isomorfismo, el conjunto de generadores $\mathbb{Z}/n\mathbb{Z}$ se identifica con el conjunto $R_n \subset \mu$, de todas las raíces n-ésimas primitivas de la unidad ($R_n = \{\varepsilon \in \mu_n$ tales que $\varepsilon^m \neq 1$ para cada $m < n\}$). El conjunto de generadores de $\mathbb{Z}/n\mathbb{Z}$ se identifica con los invertibles de $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{k} \in \mathbb{Z}/n\mathbb{Z}, (k,n) = 1\}$. Luego,

$$R_n = \{\varepsilon_n^k = cos\,\frac{2k\pi}{n} + isen\,\frac{2k\pi}{n} \text{ con } 0 < k < n \text{ y } (k,n) = 1\}$$

10. Definición : Para cada $n \in \mathbb{N}$ se denomina n-ésimo **polinomio ciclotómico** al polinomio mónico

$$\Phi_n(x) = \prod_{k<n,\,(k,n)=1} (x - \varepsilon_k)$$

11. Teorema : *Los polinomios ciclotómicos son polinomios mónicos con coeficientes enteros,*

$$\Phi_n(x) \in \mathbb{Z}[x]$$

y son irreducibles.

Demostración. Una raíz n-ésima de la unidad es primitiva si y sólo si no es d-ésima para ningún divisor estricto d de n y, por tanto,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d<n,\,d|n} \Phi_d(x)}$$

luego por recurrencia se demuestra que $\Phi_n(x)$ es mónico y además $\Phi_n(x) \in \mathbb{Z}[x]$ (obsérvese que $\Phi_1(x) = x - 1$).

Irreducibilidad: Sea $\Phi_n(x) = P(x) \cdot Q(x)$ con $P(x) \in \mathbb{Z}[x]$ primo. Como se sabe, si ε es una raíz primitiva de la unidad, entonces las raíces primitivas n-ésimas de la unidad son exactamente las de la forma ε^m con $(m,n) = 1$. Por tanto, para ver que $P(x) = \Phi_n(x)$ basta ver que si ε es raíz de $P(x)$ y p un número primo no divisor de n, entonces ε^p es también raíz de $P(x)$. Sea pues ε una raíz de $P(x)$ tal que ε^p sea raíz de $Q(x)$. Entonces, los polinomios $P(x)$ y $Q(x^p)$ tienen en común la raíz ε. Por tanto, $Q(x^p) = P(x) \cdot H(x)$. Ahora bien, pasando los coeficientes a $\mathbb{Z}/p\mathbb{Z}$, por el lema 3.3.12 que sigue, $\overline{\Phi_n(x)}^p = \overline{\Phi_n(x^p)} = \overline{P(x^p)} \cdot \overline{Q(x^p)} = \overline{P(x)}^p \cdot \overline{P(x)} \cdot \overline{H(x)} = \overline{P(x)}^{p+1}\overline{H(x)}$, luego $\overline{\Phi_n(x)}^p$ tiene raíces con multiplicidad por lo menos $p+1$. Sin embargo, $\overline{\Phi_n(x)}$ tiene las raíces distintas, pues es divisor de $x^n - 1$ cuya derivada es $nx^{n-1} \neq 0$, es decir, son primos entre sí y, por tanto de raíces distintas. Luego las raíces de $\overline{\Phi_n(x)}^p$ tienen multiplicidad p y se llega a contradicción. □

12. Lema : *Para cada $P(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ se verifica la identidad:*

$$P(x)^p = P(x^p)$$

Demostración. Para cada $a \in \mathbb{Z}/p\mathbb{Z}$ es $a^p = a$ y $(P(x) + Q(x))^p = P(x)^p + Q(x)^p$, para cada $P(x), Q(x) \in \mathbb{Z}/p\mathbb{Z}[x]$, luego

$$P(x)^p = (a_0 + a_1 x + \cdots a_n x^n)^p = a_0^p + a_1^p x^p + \cdots a_n^p (x^p)^n = P(x^p)$$

□

13. Teorema: *Sea $\mathbb{Q}(\varepsilon_n)$ el cuerpo de descomposición de $x^n - 1$. Entonces, se cumple que*

1. $\mathbb{Q}(\varepsilon_n) = \mathbb{Q}[x]/(\Phi_n(x))$.
2. *El grupo de Galois de $\mathbb{Q}(\varepsilon_n)$ es isomorfo a $(\mathbb{Z}/n\mathbb{Z})^*$.*

Demostración. 1. $\Phi_n(x)$ es un polinomio mónico irreducible en $\mathbb{Z}[x]$, luego por el teorema de Gauss es irreducible en $\mathbb{Q}[x]$. Por tanto, $\Phi_n(x)$ es el polinomio con coeficiente en $\mathbb{Q}$ mínimo anulador de ε_n. Luego, $\mathbb{Q}[x]/(\Phi_n(x)) = \mathbb{Q}(\varepsilon_n)$.

2. Si $\tau \in \mathrm{Aut}_{\mathbb{Q}-alg}(\mathbb{Q}(\varepsilon_n))$, entonces $\tau(\varepsilon_n) = \varepsilon_n^k$, para cierto $0 < k < n$, cumpliendo $(k, n) = 1$ y τ queda determinado por este exponente k. Es decir, el morfismo de grupos $\mathrm{Aut}_{\mathbb{Q}-alg}(\mathbb{Q}(\varepsilon_n)) \to (\mathbb{Z}/n\mathbb{Z})^*$, $\tau \mapsto \bar{k}$ es inyectivo. Por órdenes, ha de ser epiyectivo, luego es un isomorfismo.

□

3.3.2. Cuerpos finitos

14. Definición: Diremos que un cuerpo es finito si tiene un número finito de elementos.

Observemos que la característica de un cuerpo finito K es un número primo $p > 0$, porque el morfismo $\mathbb{Z} \to K$, $n \mapsto n$, tiene núcleo no nulo, que ha de ser un $p\mathbb{Z}$, con $p > 0$, primo. Por tanto, K es una $\mathbb{Z}/p\mathbb{Z}$ extensión finita de cuerpos. Sea $n = \dim_{\mathbb{Z}/p\mathbb{Z}} K$, entonces K es isomorfo como espacio vectorial a $(\mathbb{Z}/p\mathbb{Z})^n$, luego

$$\#K = p^n$$

Consideremos el grupo conmutativo $K^* = K - \{0\}$ con la multiplicación. Como $\#K^* = p^n - 1$, se tiene que para todo $\alpha \in K^*$, $\alpha^{p^n - 1} = 1$. Por tanto, para todo $\alpha \in K$, $\alpha^{p^n} = \alpha$. Es decir, K coincide con el conjunto de todas las raíces del polinomio de grado p^n, $x^{p^n} - x$. Polinomio que es separable. Así pues, K es el cuerpo de descomposición de $x^{p^n} - x$ y es una $\mathbb{Z}/p\mathbb{Z}$-extensión de Galois.

Hemos probado el siguiente teorema.

15. Teorema: *Sea $p > 0$ primo y $n > 0$. Entonces, sólo existe un cuerpo finito (salvo isomorfismos) de orden p^n, que denotaremos $\mathbb{F}_{p^n}$, y es precisamente el conjunto de las raíces (en el cierre algebraico de $\mathbb{F}_p$) del polinomio $x^{p^n} - x$. Luego, $\mathbb{F}_{p^n}$ es el cuerpo de descomposición de $x^{p^n} - x$, y los cuerpos finitos son extensiones de Galois de $\mathbb{F}_p$.*

16. Proposición: *$\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} - \{0\}$ es un grupo (multiplicativo) cíclico.*

Demostración. Basta ver que existe $\alpha \in \mathbb{F}_{p^n}^*$ de orden $p^n - 1$. Basta ver que el anulador del grupo conmutativo (multiplicativo) $\mathbb{F}_{p^n}^*$ es $p^n - 1$. Sea d el anulador de $\mathbb{F}_{p^n}^*$. Se verifica que d es un divisor de $p^n - 1$ y que $\alpha^d = 1$, para todo $\alpha \in \mathbb{F}_{p^n}^*$. Por tanto, $\mathbb{F}_{p^n}^*$ es un subconjunto del conjunto de raíces de $x^d - 1$, luego

$$\#\mathbb{F}_{p^n} \leq d + 1 \leq p^n$$

y por tanto $d = p^n - 1$. □

En consecuencia, $\mathbb{F}_{p^n}^* =< \alpha >$, luego $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, es decir,

$$\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(p(x))$$

siendo $p(x)$ un polinomio irreducible sobre $\mathbb{F}_p$ de grado n.

17. Definición : Sea K un cuerpo de característica $p > 0$. Llamaremos *automorfismo de Frobenius* al automorfismo de $\mathbb{F}_p$-álgebras

$$F\colon K \to K$$

definido por $F(\lambda) = \lambda^p$.

18. Teorema : *Sea $k \to K$ una extensión finita entre cuerpos finitos. Sea $k = \mathbb{F}_{p^n}$. El grupo de automorfismos,* $\mathrm{Aut}_{k-alg}\, K$*, es un grupo cíclico generado por la potencia n-ésima del automorfismo de Frobenius,*

$$\mathrm{Aut}_{k-alg}\, K =< F^n >$$

Demostración. F^n sobre $k = \mathbb{F}_{p^n}$ es el morfismo identidad. Si K es una k-extensión de grado m, $\#K = (\#k)^m = p^{nm}$. Entonces $K = \mathbb{F}_{p^{nm}}$. El orden de F^n (como automorfismo de K) es m, por tanto

$$\#\langle F^n \rangle = m = \dim_k K$$

Por tanto, K es una extensión de Galois de grupo $\langle F^n \rangle$.

□

3.4. Equivalencia de Galois

1. Notación : Dado un anillo A y un subgrupo $G \subseteq \mathrm{Aut}_{anillos}(A)$, definimos los invariantes de A por G, que denotamos A^G, como el subanillo

$$A^G := \{a \in A\colon g(a) = a, \text{ para todo } g \in G\}$$

2. Lema : *Sea A una k-álgebra, $G \subseteq \mathrm{Aut}_{k-alg}(A)$ un grupo finito de automorfismos de A y B una k-álgebra. Entonces,*

$$(A \otimes_k B)^G = A^G \otimes_k B.$$

Demostración. $B = \oplus_I k$ como k-espacio vectorial. Es fácil comprobar que

$$(A \otimes_k B)^G = (A \otimes_k (\oplus_I k))^G = (\oplus_I A)^G = \oplus_I A^G = A^G \otimes_k B$$

□

3. Teorema de Artin: *Sea K un cuerpo y $G \subseteq \mathrm{Aut}_{anillos}(K)$ un subgrupo. Entonces, K es una K^G-extensión de Galois de grupo G. Si K es una k-extensión de Galois de grupo G, entonces $K^G = k$.*

Demostración. Consideremos el morfismo de K-álgebras $\phi\colon K \otimes_{K^G} K \to \prod^G K$, $\phi(a \otimes b) = (g(a) \cdot b)_{g \in G}$. Veamos que ϕ es inyectivo. Sea $a_1 \otimes b_1 + \cdots + a_n \otimes b_n \in \mathrm{Ker}\,\phi$ un elemento no nulo con el mínimo número de sumandos. Multiplicando por $a_1^{-1} \otimes 1$, podemos suponer que $a_1 = 1$. G opera de modo natural en $K \otimes_{K^G} K$: $h(a \otimes b) := h(a) \otimes b$, para todo $h \in G$ y en $\prod^G K$ como sigue: $h((\lambda_g)_{g \in G}) = (\lambda_g)_{gh^{-1} \in G}$. Observemos que $h \circ \phi = \phi \circ h$, luego $h(\mathrm{Ker}\,\phi) = \mathrm{Ker}\,\phi$. Por lo tanto,

$$\sum_i a_i \otimes b_i - h(\sum_i a_i \otimes b_i) = (a_2 - h(a_2)) \otimes b_2 + \cdots + (a_n - h(a_n)) \otimes b_n \in \mathrm{Ker}\,\phi$$

Luego, $a_i - h(a_i) = 0$, para todo i y $\sum_i a_i \otimes b_i \in (\operatorname{Ker}\phi)^G$. Pero $(K \otimes_{K^G} K)^G = K^G \otimes_{K^G} K = K$ es un cuerpo, luego $0 = \operatorname{Ker}\phi \cap (K \otimes_{K^G} K)^G = (\operatorname{Ker}\phi)^G$. Luego, $\sum_i a_i \otimes b_i = 0$ y $\operatorname{Ker}\phi = 0$.

Por tanto, $\dim_{K^G} K = \dim_K (K \otimes_{K^G} K) \leq \dim_K \prod^G K = \#G$. Luego, K es una K^G-extensión de Galois de grupo G.

Si K es una k-extensión de Galois de grupo G, entonces $\#G = \dim_k K = \dim_k K^G \cdot \dim_{K^G} K = \dim_k K^G \cdot \#G$, luego $\dim_k K^G = 1$ y $k = K^G$.

□

4. Lema: *Sea K una k-extensión de Galois y $K' \subseteq K$ una k-subextensión. Entonces, K es una K'-extensión de Galois.*

Demostración. $K \otimes_{K'} K$ es una K-álgebra trivial porque es cociente de la K-álgebra trivial $K \otimes_k K$. Por tanto, K es una K'-extensión de Galois.

□

5. Teorema de Galois: *Sea K una k-extensión de Galois de grupo G. La asignación*

$$[\textit{Conjunto de subgrupos de } G] \to [\textit{Conjunto de } k\textit{-subextensiones de } K]\,,\ H \mapsto K^H$$

es biyectiva.

Demostración. Si $K^H = K^{H'}$, entonces $H = \operatorname{Aut}_{K^H - alg} K = \operatorname{Aut}_{K^{H'} - alg} K = H'$. Luego la asignación es inyectiva.

Sea $K' \hookrightarrow K$ una k-subextensión. Sea $H := \operatorname{Aut}_{K' - alg} K \subseteq \operatorname{Aut}_{k-alg} K$. Por la proposición anterior y el teorema de Artin, $K^H = K'$. Luego la asignación es epiyectiva.

□

6. Teorema de prolongación: *Sea K una k-extensión de Galois de grupo G y $K' = K^H \subseteq K$ una k-subextensión. Entonces,* $\operatorname{Hom}_{k-alg}(K^H, K) = G/H$.

Demostración. Denotemos $i\colon K^H \hookrightarrow K$ la inclusión natural. El morfismo natural $G/H \to \operatorname{Hom}_{k-alg}(K^H, K)$, $\bar{g} \mapsto g \circ i$ es inyectivo, porque si $g \circ i = g' \circ i$, entonces $i = (g^{-1} \circ g') \circ i$, luego $g^{-1} \circ g \in H$ y $\bar{g} = \overline{g'}$.

Para demostrar que es epiyectivo sólo tenemos que probar que $\#\operatorname{Hom}_{k-alg}(K^H, K) = \#G/\#H$.

Observemos que $\dim_k K^H = \#(G/H)$, porque $\dim_{K^H} K = \#H$, $\dim_k K = \#G$ y $\dim_k K = \dim_k K^H \cdot \dim_{K^H} K$.

K trivializa a K^H, luego $\#G/\#H = \dim_k K^H = \#\operatorname{Hom}_{k-alg}(K^H, K)$.

□

7. Definición: Sea $H \subseteq G$ un subgrupo. Llamaremos normalizador de H en G, que denotaremos $N_G(H)$, al subgrupo de G

$$N_G(H) := \{g \in G\colon gHg^{-1} = H\}$$

El normalizador de H en G es el máximo subgrupo de G en el que H es normal.

8. Proposición: *Sea K una k-extensión de Galois de grupo G y $H \subseteq G$ un subgrupo. Entonces,*

$$\operatorname{Aut}_{k-alg} K^H = N_G(H)/H$$

Por tanto, K^H es una k-extensión de Galois si y sólo si H es normal en G.

Demostración. Denotemos $i\colon K^H \hookrightarrow K$ la inclusión natural. Observemos que

$$\mathrm{Aut}_{k-alg}\, K^H = \{f \in \mathrm{Hom}_{k-alg}(K^H, K)\colon f(K^H) = K^H\},\ \tau \mapsto i \circ \tau$$

Por el teorema de prolongación, $G/H = \mathrm{Hom}_{k-alg}(K^H, K)$, $\bar{g} \mapsto g \circ i$. Por tanto,

$$\mathrm{Aut}_{k-alg}\, K^H = \{\bar{g} \in G/H\colon g(K^H) = K^H\}$$

Ahora bien, $g(K^H) = K^{gHg^{-1}}$, luego $K^H = g(K^H)$ si y sólo si $gHg^{-1} = H$, es decir, $g \in N_G(H)$. En conclusión,

$$\mathrm{Aut}_{k-alg}\, K^H = N_G(H)/H$$

□

3.5. Biografía de Galois

GALOIS BIOGRAPHY

Evariste Galois' father Nicholas Gabriel Galois and his mother Adelaide Marie Demante were both intelligent and well educated in philosophy, classical literature and religion. However there is no sign of any mathematical ability in any of Galois' family. His mother served as Galois' sole teacher until he was 12 years old. She taught him Greek, Latin and religion where she imparted her own scepticism to her son. Galois' father was an important man in the community and in 1815 he was elected mayor of Bourg-la-Reine.

The starting point of the historical events which were to play a major role in Galois' life is surely the storming of the Bastille on 14 July 1789. From this point the monarchy of Louis 16th was in major difficulties as the majority of Frenchmen composed their differences and united behind an attempt to destroy the privileged establishment of the church and the state.

Despite attempts at compromise Louis 16th was tried after attempting to flee the country. Following the execution of the King on 21 January 1793 there followed a reign of terror with many political trials. By the end of 1793 there were 4595 political prisoners held in Paris. However France began to have better times as their armies, under the command of Napoleon Bonaparte, won victory after victory.

Napoleon became first Consul in 1800 and then Emperor in 1804. The French armies continued a conquest of Europe while Napoleon's power became more and more secure. In 1811 Napoleon was at the height of his power. By 1815 Napoleon's rule was over. The failed Russian campaign of 1812 was followed by defeats, the Allies entering Paris on 31 March 1814. Napoleon abdicated on 6 April and Louis XVIII was installed as King by the Allies. The year 1815 saw the famous one hundred days. Napoleon entered Paris on March 20, was defeated at Waterloo on 18 June and abdicated for the second time on 22 June. Louis XVIII was reinstated as King but died in September 1824, Charles X becoming the new King.

Galois was by this time at school. He had enrolled at the Lycée of Louis-le-Grand as a boarder in the 4 th class on 6 October 1823. Even during his first term there was a minor rebellion and 40 pupils were expelled from the school. Galois was not involved and during 1824-25 his school record is good and he received several prizes. However in 1826 Galois was asked to repeat the year because his work in rhetoric was not up to the required standard.

February 1827 was a turning point in Galois' life. He enrolled in his first mathematics class, the class of M. Vernier. He quickly became absorbed in mathematics and his director of studies wrote

It is the passion for mathematics which dominates him, I think it would be best for him if his parents would allow him to study nothing but this, he is wasting his time here and does nothing but torment his teachers and overwhelm himself with punishments.

Galois' school reports began to describe him as singular, bizarre, original and closed. It is interesting that perhaps the most original mathematician who ever lived should be criticised for being original. M. Vernier reported however

Intelligence, marked progress but not enough method.

In 1828 Galois took the examination of the École Polytechnique but failed. It was the leading University of Paris and Galois must have wished to enter it for academic reasons. However, he also wished to enter this school because of the strong political movements that existed among its students, since Galois followed his parents example in being an ardent republican.

Back at Louis-le-Grand, Galois enrolled in the mathematics class of Louis Richard. However he worked more and more on his own researches and less and less on his schoolwork. He studied Legendre's Géométrie and the treatises of Lagrange. As Richard was to report

This student works only in the highest realms of mathematics.

In April 1829 Galois had his first mathematics paper published on continued fractions in the Annales de mathématiques. On 25 May and 1 June he submitted articles on the algebraic solution of equations to the Académie des Sciences. Cauchy was appointed as referee of Galois' paper.

Tragedy was to strike Galois for on 2 July 1829 his father committed suicide. The priest of Bourg-la-Reine forged Mayor Galois' name on malicious forged epigrams directed at Galois' own relatives. Galois' father was a good natured man and the scandal that ensued was more than he could stand. He hanged himself in his Paris apartment only a few steps from Louis-le-Grand where his son was studying. Galois was deeply affected by his father's death and it greatly influenced the direction his life was to take.

A few weeks after his father's death, Galois presented himself for examination for entry to the École Polytechnique for the second time. For the second time he failed, perhaps partly because he took it under the worst possible circumstances so soon after his father's death, partly because he was never good at communicating his deep mathematical ideas. Galois therefore resigned himself to enter the École Normale, which was an annex to Louis-le-Grand, and to do so he had to take his Baccalaureate examinations, something he could have avoided by entering the École Polytechnique.

He passed, receiving his degree on 29 December 1829. His examiner in mathematics reported:

This pupil is sometimes obscure in expressing his ideas, but he is intelligent and shows a remarkable spirit of research.

His literature examiner reported:

This is the only student who has answered me poorly, he knows absolutely nothing. I was told that this student has an extraordinary capacity for mathematics. This astonishes me greatly, for, after his examination, I believed him to have but little intelligence.

Galois sent Cauchy further work on the theory of equations, but then learned from Bulletin de Férussac of a posthumous article by Abel which overlapped with a part of his work. Galois then took Cauchy's advice and submitted a new article On the condition that an equation be soluble by radicals in February 1830. The paper was sent to Fourier, the secretary of the Paris Academy, to be considered for the Grand Prize in mathematics. Fourier died in April 1830 and Galois' paper was never subsequently found and so never considered for the prize.

Galois, after reading Abel and Jacobi's work, worked on the theory of elliptic functions and abelian integrals. With support from Jacques Sturm, he published three papers in Bulletin de Férussac in April 1830. However, he learnt in June that the prize of the Academy would be awarded the Prize jointly to Abel (posthumously) and to Jacobi, his own work never having been considered.

July 1830 saw a revolution. Charles 10th fled France. There was rioting in the streets of Paris and the director of École Normale, M. Guigniault, locked the students in to avoid them taking part. Galois tried to scale the wall to join the rioting but failed. In December 1830 M. Guigniault wrote newspaper articles attacking the students and Galois wrote a reply in the Gazette des Écoles, attacking M. Guigniault for his actions in locking the students into the school. For this letter Galois was expelled and he joined the Artillery of the National Guard, a Republican branch of the militia. On 31 December 1830 the Artillery of the National Guard was abolished by Royal Decree since the new King Louis-Phillipe felt it was a threat to the throne.

Two minor publications, an abstract in Annales de Gergonne (December 1830) and a letter on the teaching of science in the Gazette des Écoles (2 January 1831) were the last publications during his life. In January 1831 Galois attempted to return to mathematics. He organised some mathematics classes in higher algebra which attracted 40 students to the first meeting but after that the numbers quickly fell off. Galois was invited by Poisson to submit a third version of his memoir on equation to the Academy and he did so on 17 January.

On 18 April Sophie Germain wrote a letter to her friend the mathematician Libri which describes Galois' situation.

.. the death of M. Fourier, have been too much for this student Galois who, in spite of his impertinence, showed signs of a clever disposition. All this has done so much that he has been expelled form École Normale. He is without money... . They say he will go completely mad. I fear this is true.

Late in 1830 19 officers from the Artillery of the National Guard were arrested and charged with conspiracy to overthrow the government. They were acquitted and on 9 May 1831 200 republicans gathered for a dinner to celebrate the acquittal. During the dinner Galois raised his glass and with an open dagger in his hand appeared to make threats against the King, Louis-Phillipe. After the dinner Galois was arrested and held in Sainte-Pélagie prison. At his trial on 15 June his defence lawyer claimed that Galois had said

To Louis-Phillipe, if he betrays

but the last words had been drowned by the noise. Galois, rather surprisingly since he essentially repeated the threat from the dock, was acquitted.

The 14th of July was Bastille Day and Galois was arrested again. He was wearing the uniform of the Artillery of the National Guard, which was illegal. He was also carrying a loaded rifle, several pistols and a dagger. Galois was sent back to Sainte-Pélagie prison. While in prison he received a rejection of his memoir. Poisson had reported that:

His argument is neither sufficiently clear nor sufficiently developed to allow us to judge its rigour.

He did, however, encourage Galois to publish a more complete account of his work. While in Sainte-Pélagie prison Galois attempted to commit suicide by stabbing himself with a dagger but the other prisoners prevented him. While drunk in prison he poured out his soul

Do you know what I lack my friend? I confide it only to you: it is someone whom I can love and love only in spirit. I have lost my father and no one has ever replaced him, do you hear me...?

In March 1832 a cholera epidemic swept Paris and prisoners, including Galois, were transferred to the pension Sieur Faultrier. There he apparently fell in love with Stephanie-Felice du Motel, the daughter of the resident physician. After he was released on 29 April Galois exchanged letters with Stephanie, and it is clear that she tried to distance herself from the affair.

The name Stephanie appears several times as a marginal note in one of Galois' manuscripts.

Galois fought a duel with Perscheux d'Herbinville on 30 May, the reason for the duel not being clear but certainly linked with Stephanie.

You can see a note in the margin of the manuscript that Galois wrote the night before the duel.

The note reads

There is something to complete in this demonstration. I do not have the time. (Author's note).

It is this which has led to the legend that he spent his last night writing out all he knew about group theory. This story appears to have been exaggerated.

Galois was wounded in the duel and was abandoned by d'Herbinville and his own seconds and found by a peasant. He died in Cochin hospital on 31 May and his funeral was held on 2 June. It was the focus for a Republican rally and riots followed which lasted for several days.

Galois' brother and his friend Chevalier copied his mathematical papers and sent them to Gauss, Jacobi and others. It had been Galois' wish that Jacobi and Gauss should give their opinions on his work. No record exists of any comment these men made. However the papers reached Liouville who, in September 1843, announced to the Academy that he had found in Galois' papers a concise solution

...as correct as it is deep of this lovely problem: Given an irreducible equation of prime degree, decide whether or not it is soluble by radicals.

Liouville published these papers of Galois in his Journal in 1846.

The theory that Galois outlined in these papers is now called Galois theory.

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/)

3.6. Problemas

1. Si $A = \mathbb{Q}(\sqrt[3]{2})$, hallar una extensión finita L de $\mathbb{Q}$ tal que $A \otimes_{\mathbb{Q}} L = \oplus L$.

   Igualmente cuando $A = \mathbb{Q}(\sqrt[4]{2})$ y $A = \mathbb{Q}(i) \oplus \mathbb{Q}(\sqrt[3]{2})$.

2. Sea k un cuerpo de característica positiva p y sea $k \to L$ una extensión finita separable. Si $\alpha \in L$ demostrar que $k(\alpha) = k(\alpha^p)$.

3. Sea k un cuerpo de característica nula. Si A y B son dos k-álgebras finitas reducidas, probar que $A \otimes_k B$ también es una k-álgebra finita reducida.

4. Sea $k = \mathbb{F}_2(t)$ el cuerpo de las fracciones racionales en una indeterminada con coeficientes en $\mathbb{F}_2$. Demostrar que polinomio $p(x) = x^2 - t$ es irreducible en $k[x]$.

   Si $\alpha = \sqrt{t}$ es una raíz de $p(x)$, probar que $x^2 - t = (x - \alpha)^2$.

   Concluir que la extensión finita $k \to k(\sqrt{t})$ no es separable.

5. El grupo de Galois sobre $\mathbb{C}$ de cualquier polinomio separable con coeficientes complejos es trivial: $G = 1$.

6. Si un polinomio separable con coeficientes reales tiene todas sus raíces reales, entonces su grupo de Galois sobre $\mathbb{R}$ es trivial: $G = 1$. Por el contrario, si tiene alguna raíz imaginaria, entonces su cuerpo de descomposición sobre $\mathbb{R}$ es $L = \mathbb{C}$, y su grupo de Galois es $G = \{\mathrm{id}, \tau\}$, donde τ denota la conjugación compleja.

7. Determinar cuáles de las siguientes extensiones de $\mathbb{Q}$ son de Galois y, en caso afirmativo, determinar su grupo de automorfismos:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \quad , \quad \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) \quad , \quad \mathbb{Q}(i\sqrt{2}, \sqrt[3]{3}) \quad , \quad \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$$

8. Determinar el cuerpo de descomposición L sobre $\mathbb{Q}$ del polinomio $p(x) = x^4 - 4$ y su grupo de Galois. Análogamente para el polinomio $p(x) = (x^2 - 2)(x^2 + 1)$.

9. Sea $p_2(x) = ax^2 + bx + c \in k[x]$ un polinomio separable de grado 2. Si $p_2(x)$ tiene alguna raíz en k, entonces su grupo de Galois sobre k es $G = \{\mathrm{id}\}$.

   Si $p_2(x)$ no tiene raíces en k, lo que equivale a que sea irreducible en $k[x]$, entonces su grupo de Galois sobre k es $G = S_2$.

10. Probar que toda extensión de Galois $k \to L$ es el cuerpo de descomposición sobre k de algún polinomio separable con coeficientes en k.

11. Sea n un número natural, $n \geq 2$. Determinar el grado y el grupo de automorfismos de $\mathbb{Q}(\sqrt[n]{2})$ sobre $\mathbb{Q}$. ¿Cuándo es $\mathbb{Q}(\sqrt[n]{2})$ una extensión de Galois de $\mathbb{Q}$? ¿Es $\mathbb{Q}(\sqrt[4]{2})$ una extensión de Galois de $\mathbb{Q}(\sqrt{2})$?

12. Determinar el grupo de automorfismos de $\mathbb{Q}(\sqrt[8]{2}, i)$ sobre $\mathbb{Q}$. ¿Es $\mathbb{Q}(\sqrt[8]{2}, i)$ una extensión de Galois de $\mathbb{Q}$?

13. Si $k \to L$ y $k \to L'$ son dos extensiones de Galois de un mismo cuerpo k, probar que cualquier compuesto $L'L$ también es una extensión de Galois de k. Concluir que todos los compuestos de L con L' son isomorfos, y que $L \otimes_k L'$ descompone en suma directa de extensiones de k isomorfas entre sí.

14. Sean $k \to L$ y $k \to L'$ dos extensiones de Galois de un mismo cuerpo k, de grupos G y G' respectivamente. Si $L \otimes_k L'$ es un cuerpo, demostrar que es una extensión de Galois de k y que su grupo de Galois es isomorfo a $G \times G'$.

15. Determinar el menor subcuerpo de $\mathbb{C}$ que contenga a $\alpha = \sqrt{2} + \sqrt[3]{2}$ y sea una extensión de Galois de $\mathbb{Q}$. Calcular su grupo de Galois. Determinar el grado del polinomio irreducible de α sobre $\mathbb{Q}$.

16. Calcular el grupo de Galois del polinomio $(x^3 + 3)(x^2 + 3)$.

17. Si el discriminante de una cúbica $p(x) \in k[x]$ (no necesariamente irreducible) es un cuadrado en k y la característica de k no es 2, probar que el grupo de Galois G de $p(x)$ sobre k es $G = A_3$ ó $G = 1$.

18. Sea K una extensión de $\mathbb{Q}$. Probar que $x^3 - 3x + 1$ es irreducible en $K[x]$ o tiene todas sus raíces en K. (*Indicación:* El discriminante es $\Delta = 9^2$).

19. Si el grupo de Galois sobre $\mathbb{Q}$ de una cúbica es A_3, probar que tiene tres raíces reales.

20. Una ecuación cúbica con coeficientes reales tiene una única raíz real cuando el discriminante es negativo, y tiene todas sus raíces reales cuando el discriminante es positivo.

21. Si Δ es el discriminante de una cúbica irreducible con coeficientes racionales, probar que su cuerpo de descomposición es $\mathbb{Q}(\sqrt{\Delta}, \alpha)$ donde α es cualquier raíz compleja.

22. Estudiar el grupo de Galois de una cúbica binómica $x^3 - a$ sobre un cuerpo k de característica 0, según que las raíces cúbicas de la unidad estén o no en k.

23. Calcular el grupo de Galois de la cúbica binómica genérica $x^3 - a$ sobre los números racionales (i.e., sobre el cuerpo $\mathbb{Q}(a)$ de funciones racionales en una indeterminada). ¿Y sobre el cuerpo de los números complejos?

24. Sea k un cuerpo de característica nula y sea $k \to L$ una extensión de Galois de grupo G. Si $H = \{\tau_1, \ldots, \tau_n\}$ es un subgrupo de G, probar que es epiyectiva la aplicación k-lineal

$$s\colon L \to L^H \quad , \quad s(\alpha) = \tau_1(\alpha) + \ldots + \tau_n(\alpha)\ .$$

25. Hallar todos los cuerpos intermedios del cuerpo de descomposición L sobre $\mathbb{Q}$ del polinomio $x^3 - 2$. Análogamente para el polinomio $(x^2 - 2)(x^2 + 1)$ y el polinomio $x^4 - 4$.

26. Demostrar que $\sqrt{3}$ no está en la extensión $\mathbb{Q}(i, \sqrt[4]{2}\,)$.

    Determinar un polinomio irreducible con coeficientes en $\mathbb{Q}(\sqrt{3}\,)$ que admita la raíz $\sqrt[4]{2}$.

27. Sea $\mathbb{Q} \to L$ una extensión de Galois. Si su grupo de Galois es el grupo de Klein $V = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, probar que $L = \mathbb{Q}(\alpha, \beta)$, donde $\alpha^2, \beta^2 \in \mathbb{Q}$.

28. Si $k \to L$ es una extensión finita separable, probar que sólo hay un número finito de cuerpos intermedios. (*Indicación:* Probarlo para la envolvente de Galois de L).

29. Sea k un cuerpo infinito. Si una extensión finita $k \to k(\alpha, \beta)$ es separable, probar que existen $a, b \in k$ tales que $k(\alpha + b\beta) = k(\alpha + a\beta)$. Concluir que $k(\alpha, \beta) = k(\alpha + a\beta)$, y que toda extensión finita separable de k está generada por un elemento.

30. Demostrar que toda extensión separable $k \to L$ de grado 2 es de Galois.

    Demostrar que toda extensión de grado 2 de un cuerpo de característica distinta de 2 es una extensión de Galois.

    ¿Puede tener un cuerpo de característica 2 una extensión de Galois de grado 2?

31. Dar un ejemplo de extensiones de Galois $k \to L'$ y $L' \to L$ de grado 2 tales que $k \to L$ no sea extensión de Galois.

32. Sea σ el automorfismo de $\mathbb{Q}(\varepsilon_5)$ tal que $\sigma(\varepsilon_5) = \varepsilon_5^4$. Probar que $\mathbb{Q}(\sqrt{5}\,)$ es el cuerpo de elementos invariantes por σ.

33. Determinar el grupo de Galois de $x^6 - 8$ sobre $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}\,)$, $\mathbb{Q}(\varepsilon_3)$, $\mathbb{Q}(\sqrt[3]{2}\,)$ y $\mathbb{Q}(\sqrt[4]{2}\,)$.

34. Para cada automorfismo τ del cuerpo $\mathbb{Q}(e^{2\pi i/8})$, calcular el grado sobre $\mathbb{Q}$ del cuerpo de invariantes $\mathbb{Q}(\varepsilon_8)^\tau = \{\alpha \in \mathbb{Q}(\varepsilon_8)\colon \tau(\alpha) = \alpha\}$.

    ¿Existe algún automorfismo de $\mathbb{Q}(\varepsilon_8)$ que sólo deje fijos los números racionales?

35. Determinar el número de extensiones de $\mathbb{Q}$ de grado 2 contenidas en $\mathbb{Q}(e^{2\pi i/n})$ en los casos $5 \le n \le 13$. Igualmente para las de grado 3.

36. Determinar todas las extensiones de $\mathbb{Q}$ contenidas en $\mathbb{Q}(e^{2\pi i/n})$ en los casos $5 \le n \le 9$.

37. Determinar los números racionales b tales que $\sqrt{b} \in \mathbb{Q}(e^{2\pi i/n})$ en los casos $5 \le n \le 9$.

38. Sea $k \to L$ una extensión de Galois de grado n. Si su grupo de Galois es cíclico, probar las siguientes afirmaciones:

a) Para cada divisor d de n, existe un único cuerpo intermedio de grado d sobre k.

b) Si L_1 y L_2 son dos cuerpos intermedios, entonces $L_1 \subseteq L_2$ si y sólo si $[L_1 : k]$ divide a $[L_2 : k]$.

39. Demostrar que $\sqrt{-3}$ no está en la extensión $\mathbb{Q}(\sqrt{-2}, i)$. Concluir que $\mathbb{Q}(\sqrt{-3}, \sqrt{-2}, i)$ es una extensión de Galois de $\mathbb{Q}$ de grado 8.

40. Probar que el grupo de Galois de $L = \mathbb{Q}(\sqrt{3}, \sqrt{2}, i)$ tiene 7 subgrupos de orden 2, y que $\mathbb{Q}(\sqrt{3}, \sqrt{2})$ es la única extensión real de grado 4 contenida en L. Concluir que $\sqrt[4]{3}$ no está en L y que $\mathbb{Q}(\sqrt[4]{3}, \sqrt{2}, i)$ es una extensión de Galois de $\mathbb{Q}$ de grado 16.

41. Probar que el grupo de Galois de $L = \mathbb{Q}(\sqrt[4]{3}, \sqrt{2}, i)$ tiene 7 subgrupos de orden 2, y que $\mathbb{Q}(\sqrt[4]{3}, \sqrt{2})$ es la única extensión real de grado 8 contenida en L.

    Si $\sqrt[8]{3} \in L$, probar que $\mathbb{Q}(\sqrt{2}, i) \to L = \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$ es una extensión cíclica de grado 4 y, aplicando el teorema fundamental de las ecuaciones cíclicas, obtener la contradicción $\sqrt{3} \in \mathbb{Q}(\sqrt{2}, i)$.

    Concluir que $\mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$ es una extensión de Galois de $\mathbb{Q}$ de grado 32.

42. Demostrar que $\mathbb{Q} \to \mathbb{Q}(\sqrt[8]{3}, i)$ no es una extensión de Galois, y que $\sqrt{2}$ no está en $\mathbb{Q}(\sqrt[8]{3}, i)$.

43. Expresar con radicales reales una raíz compleja α del polinomio $x^4 + 2$. Determinar si es cierto que $i \in \mathbb{Q}(\alpha)$ ó si $\sqrt{2} \in \mathbb{Q}(\alpha)$. Más aún, hallar todas las extensiones de $\mathbb{Q}$ de grado 2 contenidas en el cuerpo $\mathbb{Q}(\alpha)$

44. Determinar si $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$ es una extensión de Galois de $\mathbb{Q}$.

45. Hallar un polinomio con coeficientes racionales $p(x)$ que no tenga raíces racionales, pero tal que cada automorfismo $\tau \in G$ de su grupo de Galois deje fija alguna raíz de $p(x)$. (*Indicación:* Elegir una extensión de Galois $\mathbb{Q} \to L$ cuyo grupo de Galois G no sea cíclico, y para cada automorfismo $\tau_i \in G$ elegir $\alpha_i \in L - \mathbb{Q}$ tal que $\tau_i(\alpha_i) = \alpha_i$. El producto de los polinomios irreducibles de estos irracionales α_i sirve).

46. Sea $p(x) \in \mathbb{Q}[x]$ un polinomio irreducible de grado n. Probar que en su grupo de Galois G hay un automorfismo que no deja fija ninguna raíz.

    (*Indicación:* Si H_i es el subgrupo de G formado por los automorfismos que dejan fija la raíz i–ésima, entonces $|H_i| = |G|/n$ y por tanto $H_1 \cup \ldots \cup H_n \neq G$.)

47. Sea $q(x) \in k[x]$ un polinomio separable cuyas raíces, en su cuerpo de descomposición, formen un cuerpo. Demostrar que k es un cuerpo de característica positiva p y que $q(x) = x^{p^n} - x$ para algún número natural $n \geq 1$.

48. Calcular las raíces y el grupo de Galois del polinomio $x^4 - x^2 + 1$ con coeficientes en $\mathbb{F}_5$.

49. Probar que el producto de todos los polinomios mónicos e irreducibles de grado ≤ 2 con coeficientes en $\mathbb{F}_5$ es $x^{25} - x$.

50. Probar que todo polinomio irreducible de grado 2 con coeficientes en $\mathbb{F}_p$ tiene sus raíces en el cuerpo $\mathbb{F}_{p^2}$, y que todo elemento de $\mathbb{F}_{p^2}$ es raíz de un polinomio irreducible de grado 1 ó 2. Concluir que el número de polinomios mónicos irreducibles de grado 2 con coeficientes en $\mathbb{F}_p$ es $(p^2 - p)/2$. ¿Cuál es el número de polinomios irreducibles en $\mathbb{F}_p[x]$ de grado 2?

51. Hallar el número de polinomios mónicos irreducibles de grado 3 con coeficientes en $\mathbb{F}_p$. Análogamente para los de grado 4, 6 y 8.

52. Sea $p \neq 2$ un número primo. Probar que el núcleo del morfismo de grupos $\mathbb{F}_p^* \to \mathbb{F}_p^*$ $\bar{a} \mapsto \bar{a}^2$ es $\{\pm 1\}$ y concluir que tenemos un isomorfismo de grupos $\mathbb{F}_p^*/\mathbb{F}_p^{*2} = \{\pm 1\}$.

    Probar que la proyección canónica $\mathbb{F}_p^* \to \mathbb{F}_p^*/\mathbb{F}_p^{*2} = \{\pm 1\}$ transforma cada clase $\bar{a} \in \mathbb{F}_p^*$ en el símbolo de Legendre $\left(\frac{a}{p}\right)$ y concluir que éste es multiplicativo: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

53. Sean $p < q$ dos números primos distintos. Probar que p es resto cuadrático módulo q si y sólo si p genera en $\mathbb{F}_q^*$ un subgrupo de índice par.

54. Probar que el polinomio $(x^2 + 1)(x^2 - 2)(x^2 + 2)$ tiene raíz en $\mathbb{F}_p$ para todo número primo p, aunque carezca de raíces racionales.

55. Sean p, q dos números primos distintos. Probar que las siguientes condiciones son equivalentes:

    a) $x^q - 1$ tiene alguna raíz $x \neq 1$ en $\mathbb{F}_{p^n}$.

    b) $x^q - 1$ tiene q raíces distintas en $\mathbb{F}_{p^n}$.

    c) $p^n - 1$ es múltiplo de q.

56. Sean p, q dos números primos distintos. Probar que p genera el grupo cíclico $(\mathbb{Z}/q\mathbb{Z})^*$ si y sólo si el polinomio $x^{q-1} + \ldots + x + 1$ es irreducible en $\mathbb{F}_p[x]$.

57. Sea $p > 3$ un número primo. Probar que

$$\sqrt{3} = \varepsilon_{12}^3(2\varepsilon_{12}^4 + 1) = \varepsilon_{12}^3 + 2\varepsilon_{12}^7 \in \mathbb{F}_p(\varepsilon_{12}) \, .$$

    y concluir (sin usar la Ley de reciprocidad cuadrática) que 3 es resto cuadrático módulo p si y sólo si $p \equiv 1$ ó -1 (mód. 12).

58. Sea $q \neq 2$ un número primo. Probar que $\sqrt{q} \in \mathbb{F}_p(\varepsilon_{4q})$.

59. Si $\mathbb{F}_q$ es un cuerpo finito de característica distinta de 2, probar que el número de cuadrados en $\mathbb{F}_q$ es $(q + 1)/2$. Concluir que todo elemento a de un cuerpo finito descompone en suma de dos cuadrados.

    (*Indicación:* Si Q es el conjunto de cuadrados, probar que $Q \cap (a - Q)$ no es vacío).

60. Demostrar que la norma $N\colon \mathbb{F}_{p^n}^* \to \mathbb{F}_p^*$, $N(a) = F(a)F^2(a) \ldots F^n(a)$, es un morfismo de grupos epiyectivo, donde F denota el automorfismo de Frobënius $F(\alpha) = \alpha^p$.

    (*Indicación:* Estudiar el orden del núcleo de la norma).

61. Sean a, b números enteros y sea p un número primo. Si $-4a^3 - 27b^2$ no es un resto cuadrático módulo p, probar que la congruencia $x^3 + ax \equiv b$ (módulo p) admite alguna solución entera.

62. Sean $k \to L'$ y $L' \to L$ dos extensiones de Galois. Si todo automorfismo de L' sobre k puede extenderse a un automorfismo de L, probar que $k \to L$ es una extensión de Galois.

    (*Indicación:* Considerar el morfismo de restricción $\mathrm{Aut}_{k-alg}L \to \mathrm{Aut}_{k-alg}L'$.)

63. Sea $k \to L$ una extensión de Galois de grupo G y sean K_1, K_2 dos cuerpos intermedios. Demostrar que si existe un isomorfismo de k-álgebras $f\colon K_1 \to K_2$, entonces existe algún automorfismo $\sigma \in G$ tal que $\sigma(K_1) = K_2$.

64. Sea $k \to L$ una extensión de Galois de grupo G y sean K_1, K_2 dos cuerpos intermedios. Demostrar que $K_1 \simeq K_2$ si y sólo si los subgrupos de G correspondientes a K_1 y K_2 son conjugados.

65. Si $k \to L'$ y $L' \to L$ son extensiones de Galois, entonces $k \to L$ es extensión de Galois:

$$L' \otimes_k L = L' \otimes_k L' \otimes_{L'} L = (\oplus L') \otimes_{L'} L = \oplus L$$
$$L \otimes_k L = L \otimes_{L'} (L' \otimes_k L) = L \otimes_{L'} (\oplus L) = \oplus(L \otimes_{L'} L) = \oplus(\oplus L)$$

¿Qué parte del razonamiento es falaz?

Capítulo 4

Aplicaciones de la teoría de Galois

4.1. Grupo simétrico

El grupo simétrico S_n es el grupo de todas las biyecciones (o "permutaciones") de un conjunto de n-elementos en sí mismo, con la operación composición de aplicaciones.

Comentario: Una biyección entre dos conjuntos $\tau\colon X \to Y$, puede entenderse como una identificación de X con Y: "a $x \in X$ lo llamamos $\tau(x)$ en Y". Dada una aplicación $f\colon X \to X$, que aplica x en $f(x)$, tenemos la correspondiente aplicación en Y: "la que aplica $\tau(x)$ en $\tau(f(x))$, es decir, la aplicación $\tau\circ f\circ\tau^{-1}\colon Y \to Y$". Así el grupo de las permutaciones de X se identifica con el grupo de las permutaciones de Y (vía la identificación de X con Y). Con mayor precisión, el morfismo

$$Biy\,X \to Biy\,Y, \quad \sigma \mapsto \tau\circ\sigma\circ\tau^{-1}$$

es un isomorfismo de grupos (como el lector puede comprobar).

Si Y es un conjunto de orden n, entonces Y es biyectivo con $\{1,\dots,n\} =: X$ y $Biy\,Y = Biy\,X =: S_n$. El número de permutaciones de n elementos es $n!$, luego $|S_n| = n!$.

1. Definición: Dados r elementos distintos $x_1,\dots,x_r \in X$, con $r > 1$, denotaremos $(x_1,\dots,x_r) = \sigma \in Biy\,X$ a la permutación que definida por $\sigma(x_i) = x_{i+1}$, para todo $i < r$; $\sigma(x_r) = x_1$; y $\sigma(x) = x$, para todo $x \notin \{x_1,\dots,x_r\}$. Diremos que $(x_1,\dots,x_r)$ es un ciclo y observemos que es de orden r. Si $r = 2$, diremos que el ciclo (x_1, x_2) es una transposición. Diremos que dos ciclos $(x_1,\dots,x_r), (x'_1,\dots,x'_{r'})$ de $Biy\,X$ son disjuntos si $x_i \neq x'_j$ para todo i, j.

2. Lema: *Si $\sigma = (x_1,\dots,x_r)$ y $\sigma' = (x'_1,\dots,x'_{r'})$ son disjuntos, entonces conmutan, es decir, $\sigma\circ\sigma' = \sigma'\circ\sigma$.*

Demostración. Para $x \in \{x_1,\dots,x_r\}$, $(\sigma\circ\sigma')(x) = \sigma(x) = (\sigma'\circ\sigma)(x)$. Para $x \in \{x'_1,\dots,x'_r\}$, $(\sigma\circ\sigma')(x) = \sigma'(x) = (\sigma'\circ\sigma)(x)$. Para $x \notin \{x_i, x'_j\}_{i,j}$, $(\sigma\circ\sigma')(x) = x = (\sigma'\circ\sigma)(x)$.

De otro modo (teniendo en cuenta el comentario anterior): $\sigma'\circ\sigma\circ\sigma'^{-1} = (\sigma'(x_1),\dots,\sigma'(x_r)) = (x_1,\dots,x_r) = \sigma$ y hemos concluido.

□

3. Teorema: *Toda permutación $\sigma \in S_n$, distinta de la identidad, es igual a un producto de ciclos disjuntos, de modo único salvo el orden de los factores.*

Demostración. Sea $x \in X$, tal que $\sigma(x) \neq x$. Sea r el mínimo número natural positivo tal que $\sigma^r(x) = x$ (tal número existe porque el orden de σ, que divide al orden de S_n, es finito). Para todo $0 \leq s < s' < r$, se cumple

que $\sigma^{s'}(x) \neq \sigma^s(x)$: pues componiendo con σ^{-s} son distintos, pues $\sigma^{s'-s}(x) \neq x$, porque $0 < s' - s < r$. Sea $\sigma_1 = (x, \sigma(x), \ldots, \sigma^{r-1}(x))$. Entonces, como σ_1 y σ coinciden sobre $\{x, \sigma(x), \ldots, \sigma^{r-1}(x)\}$ y σ_1 es la identidad sobre $X - \{x, \sigma(x), \ldots, \sigma^{r-1}(x)\}$, se cumple que $\sigma_1^{-1} \circ \sigma$ deja fijos $\{x, \sigma(x), \ldots, \sigma^{r-1}(x)\}$ y los que dejaba fijos σ. Reiterando el proceso obtenemos ciclos disjuntos $\sigma_1, \ldots, \sigma_s$ tales que $\sigma_s^{-1} \circ \cdots \circ \sigma_1^{-1} \circ \sigma = \mathrm{Id}$. Luego, $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$.

Sea otra descomposición $\sigma = \tau_1 \circ \cdots \tau_t$ en producto de ciclos disjuntos. Reordenando, podemos suponer que $\tau_1(x) \neq x$. Es decir, x "aparece" en el ciclo τ_1 (y en el de σ_1). Luego, $\tau_1(x) = \sigma(x) = \sigma_1(x)$. Obviamente, $\tau_1(x) = \sigma(x) = \sigma_1(x)$ "aparece" en ciclo de τ_1 y en el de σ_1. Luego, $\tau_1^2(x) = \sigma^2(x) = \sigma_1^2(x)$. Así sucesivamente, $\tau_1^i(x) = \sigma^i(x) = \sigma_i^2(x)$, para todo i. Por tanto, $\tau_1 = \sigma_1$ y $\sigma_2 \circ \cdots \sigma_s = \tau_2 \circ \cdots \circ \tau_t$. Reiterando el argumento concluimos que, después de reordenar los factores, $\sigma_2, \ldots, \sigma_s$ coinciden con $\tau_2, \ldots, \tau_t$.

□

4. Definición: Sea $\sigma \in S_n$ una permutación distinta de la identidad. Sea $\sigma = \sigma_1 \circ \cdots \sigma_s$ una descomposición en producto de ciclos disjuntos y d_i el orden de σ_i. Reordenando podemos suponer que $d_1 \geq d_2 \geq \cdots \geq d_s$. Diremos que $d_1, \ldots, d_s$ es la forma de σ.

5. Definición: Dado un elemento $g \in G$, diremos que el morfismo $\tau_g \colon G \to G$, $\tau_g(g') := gg'g^{-1}$, es la conjugación en G por g. Diremos que $h, h' \in G$ son conjugados si y sólo si existe $g \in G$, de modo que $\tau_g(h) = h'$.

6. Teorema: *La condición necesaria y suficiente para que $\sigma, \sigma' \in S_n$ sean conjugadas es que tengan la misma forma.*

Demostración. Sea $\sigma = (x_{11}, \ldots, x_{1d_1}) \circ \cdots \circ (x_{s1}, \cdots, x_{sd_s})$ una descomposición en producto de ciclos disjuntos y $\tau \in S_n$. Entonces,

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_{11}), \ldots, \tau(x_{1d_1})) \circ \cdots \circ (\tau(x_{s1}), \cdots, \tau(x_{sd_s}))$$

que tiene la misma forma. Sea $\sigma' = (x'_{11}, \ldots, x'_{1d_1}) \circ \cdots \circ (x'_{s1}, \cdots, x'_{sd_s})$. Si τ es cualquier permutación que cumpla $\tau(x_{ij}) = x'_{ij}$, para todo i, j, entonces $\tau \circ \sigma \circ \tau^{-1} = \sigma'$. □

7. Proposición: *Todo permutación $\sigma \in S_n$ es producto de transposiciones.*

Demostración. Como toda permutación es producto de ciclos, basta probar que todo ciclo es producto de transposiciones. Sea, pues, un ciclo $(x_1, \ldots, x_r) \in S_n$. Obviamente, $(x_1, x_2)(x_1, \ldots, x_r) = (x_2, \ldots, x_r)$, luego

$$(x_1, \ldots, x_r) = (x_1, x_2)(x_2, \ldots, x_r) = (x_1, x_2)(x_2, x_3)(x_3, \ldots, x_r) = \cdots = (x_1, x_2)(x_2, x_3) \cdots (x_{r-1}, x_r)$$

□

Signo de una permutación.

Suponemos que el lector sabe qué es el anillo de polinomios en n variables con coeficientes en los números racionales, que denotamos $\mathbb{Q}[x_1, \ldots, x_n]$. Sea $S_n = Biy(\{1, 2, \ldots, n\})$.

$\mathbb{Q}[x_1, \ldots, x_n]$ es de modo natural un S_n-conjunto:

$$\sigma \cdot p(x_1, \ldots, x_n) := p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

para todo $\sigma \in S_n$ y $p(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$.

Sea $\delta := \prod_{i<j}(x_i - x_j) \in \mathbb{Q}[x_1, \ldots, x_n]$. Es fácil ver que $\sigma \cdot \delta = \pm\delta$.

8. Definición: Llamaremos signo de una permutación $\sigma \in S_n$, que denotaremos $\mathrm{sign}(\sigma)$, al número entero 1 ó -1 tal que $\sigma \cdot \delta = \mathrm{sign}(\sigma) \cdot \delta$.

Es fácil ver que $\operatorname{sign}(\mathrm{Id}) = 1$ y que $\operatorname{sign}((1,2)) = -1$.

Consideremos el grupo (multiplicativo) $\{1,-1\} \subset \mathbb{Q} - \{0\}$. El morfismo natural $\operatorname{sign}\colon S_n \to \{1,-1\}$, $\sigma \mapsto \operatorname{sign}(\sigma)$, es un morfismo de grupos:

$$\operatorname{sign}(\sigma)\cdot\operatorname{sign}(\sigma')\cdot\delta = \sigma\cdot(\sigma'\cdot\delta) = (\sigma\cdot\sigma')\cdot\delta = \operatorname{sign}(\sigma\cdot\sigma')\cdot\delta$$

Luego, $\operatorname{sign}(\sigma)\cdot\operatorname{sign}(\sigma') = \operatorname{sign}(\sigma\cdot\sigma')$.

Evidentemente, sign es un epimorfismo.

9. Definición: Llamaremos sugbrupo alternado de S_n, que denotaremos A_n, al núcleo del morfismo sign, es decir, al subgrupo (normal) de S_n formado por las permutaciones de signo positivo.

Por el teorema de isomorfía $S_n/A_n \simeq \{1,-1\} \simeq \mathbb{Z}/2\mathbb{Z}$. Por el teorema de Lagrange, $|A_n| = |S_n|/2 = n!/2$ $(n > 1)$.

10. Ejercicio: Sea $n \geq 2$, $A_n \subseteq S_n$ y $\mathbb{Z}/2\mathbb{Z} = \langle(1,2)\rangle \subseteq S_n$. Probar que $S_n = A_n \rtimes \mathbb{Z}/2\mathbb{Z}$.

Observemos que el signo es invariante por conjugaciones, es decir,

$$\operatorname{sign}(\tau\sigma\tau^{-1}) = \operatorname{sign}(\tau)\cdot\operatorname{sign}(\sigma)\cdot\operatorname{sign}(\tau)^{-1} = \operatorname{sign}(\sigma)$$

En particular, el signo de toda transposición es -1, porque todas son conjugadas de la transposición $(1,2)$.

11. Proposición: *Si la forma de una permutación $\sigma \in S_n$ es $d_1,\dots,d_r$, entonces* $\operatorname{sign}(\sigma) = (-1)^{d_1-1}\cdots(-1)^{d_r-1} = (-1)^{d_1+\cdots+d_r-r}$.

Demostración. Si $\sigma = (x_1,\dots,x_r)$ es un ciclo, entonces $(x_1,\dots,x_r) = (x_1,x_2)(x_2,x_r)\cdots(x_{r-1},x_r)$ es producto de $r-1$ transposiciones. Como el morfismo sign es un morfismo de grupos, $\operatorname{sign}(\sigma) = (-1)^{r-1}$.

En general, $\sigma = \sigma_1\cdots\sigma_r$, donde σ_i es un ciclo de orden d_i. Por tanto, $\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma_1)\cdots\operatorname{sign}(\sigma_r) = (-1)^{d_1-1}\cdots(-1)^{d_r-1}$. □

4.2. Grupos resolubles

1. Definición: Se llama *serie normal* en G a cada cadena de subgrupos $1 \subset G_1 \subset \cdots \subset G_r = G$ tal que cada G_i es normal en el siguiente, G_{i+1}. Se llaman *factores* de la serie normal a los grupos G_{i+1}/G_i.

2. Definición: Se dice que un grupo G de orden finito es resoluble si contiene una serie normal de factores grupos de orden primo.

3. Proposición: *Sea $f\colon G \to G'$ un morfismo de grupos.*

a Si $H' \subseteq G'$ un subgrupo normal, entonces, $H := f^{-1}(H')$ es un subgrupo normal de G y el morfismo natural

$$\bar{f}\colon G/H \to G'/H',\ \bar{f}(\bar{g}) := \overline{f(g)}$$

es inyectivo. Además, si f es un epimorfismo, entonces $\bar{f}$ es un isomorfismo.

b Si f es un epimorfismo y $H \subseteq G$ es un subgrupo normal, entonces $f(H)$ es un subgrupo normal de G' y el morfismo natural

$$\bar{f}\colon G/H \to G'/f(H)$$

es un epimorfismo de grupos.

Demostración. a. Dado $g \in G$ y $h \in f^{-1}(H')$, entonces $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \in H'$, luego $ghg^{-1} \in H'$ y H es un subgrupo normal de G.

Si $\bar{f}(\bar{g}) = \bar{1}$, entonces $\overline{f(g)} = \bar{1}$ y $f(g) \in H'$, es decir, $g \in f^{-1}(H') = H$, que equivale a decir que $\bar{g} = \bar{1} \in G/H$. En conclusión, $\bar{f}$ es inyectivo.

Por último, supongamos que f es epiyectivo. Dado $\overline{g'} \in G'/H'$, sea $g \in G$ tal que $f(g) = g'$, entonces $\bar{f}(\bar{g}) = \overline{g'}$, $\bar{f}$ es epiyectivo, luego isomorfismo.

b. Dado $g' = f(g) \in G'$ y $h' = f(h) \in f(H)$, entonces $g' \cdot h' \cdot g'^{-1} = f(ghg^{-1}) \in f(H)$. Luego $f(H)$ es un subgrupo normal de G'. Dado $\overline{g'} \in G'/f(H')$, se tiene que $g' = f(g)$ para cierto $g \in G$, luego $\bar{f}(\bar{g}) = \overline{f(g)} = \overline{g'}$. Luego, $\bar{f}$ es un epimorfismo de grupos.

□

4. Proposición: *Sea G un grupo y $H \subseteq G$ un subgrupo normal. Entonces, G es resoluble si y sólo si H y G/H son resolubles.*

Demostración. Sea G resoluble y $1 \subset G_1 \subset \cdots \subset G_r = G$ una serie normal de factores grupos de orden primo.

La cadena $1 \subseteq G_1 \cap H \subseteq \cdots \subseteq G_r \cap H = H$ es una serie normal (considérese en 4.2.3 a. el morfismo $G_i \cap H \hookrightarrow G_i$ y el subgrupo normal $G_{i-1} \subset G_i$). Además, $(G_i \cap H)/(G_{i-1} \cap H)$ es de orden primo porque es subgrupo de G_i/G_{i-1}. Luego H es resoluble.

Sea $\pi\colon G \to G/H$ el morfismo de paso al cociente. La cadena $\bar{1} \subseteq \pi(G_1) \subseteq \cdots \subseteq \pi(G_r) = G/H$ es una serie normal (considérese en 4.2.3 b. el epimorfismo $\pi\colon G_i \to \pi(G_i)$ y el subgrupo normal $G_{i-1} \subset G_i$). Además, $\pi(G_i)/\pi(G_{i-1}$ es de orden primo porque es un cociente de G_i/G_{i-1}. Luego G/H es resoluble.

Supongamos ahora que H y G/H son resolubles. Sean $1 \subseteq H_1 \subseteq H_s = H$ y $\bar{1} \subset G'_1 \subset \cdots \subset G'_t = G/H$ series normales de factores grupos de orden primo. Sean $G_i := \pi^{-1}(G'_i)$. Entonces, G_{i-1} es normal en G_i y $G_i/G_{i-1} = G'_i/G'_{i-1}$ (considérese en 4.2.3 a. el epimorfismo $\pi\colon G_i \to G'_i$ y el subgrupo $G'_{i-1} \hookrightarrow G'_i$.

Por tanto, la cadena $1 \subseteq H_1 \subseteq H_s = H = \pi^{-1}(\bar{1}) \subset G_1 \subset \cdots \subset G_t = G$ es una serie normal de factores grupos de orden primo. En conclusión, G es resoluble.

□

5. Proposición: *Si $G_1, \ldots, G_n$ son grupos resolubles, entonces $G = G_1 \times \cdots \times G_n$ es resoluble.*

Demostración. Procedamos por inducción sobre n. Si $n = 1$ la proposición es obvia. Supongamos $n > 1$. $H = G_1 \times \cdots \times G_{n-1}$ es resoluble por hipótesis de inducción. Tenemos que probar que $H \times G_n = G_1 \times \cdots \times G_n$ es resoluble. Vía la inclusión $H \hookrightarrow H \times G_n$, $h \mapsto (h, 1)$, tenemos que H es un subrupo normal de $H \times G_n$. Además, $H \times G_n/H \simeq G_n$, $\overline{(h, g)} \mapsto g$. Por la proposición anterior, como H y G_n son resolubles, entonces $H \times G_n$ es resoluble. □

6. Proposición: *Los grupos finitos abelianos son resolubles.*

Demostración. Si G es un grupo finito abeliano entonces $G \simeq \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{n_r}$. Basta que probar que los grupos cíclicos $\mathbb{Z}/p^n\mathbb{Z}$, con p primo, son resolubles.

Tenemos la cadena

$$\bar{0} \subset \langle \overline{p^{n-1}} \rangle \subset \langle \overline{p^{n-2}} \rangle \subset \cdots \langle \overline{p} \rangle \subseteq \mathbb{Z}/p^n\mathbb{Z}$$

es una serie normal de factores grupos de orden p. Luego $\mathbb{Z}/p^n\mathbb{Z}$ es resoluble.

□

7. Proposición: *Sea $p > 0$ un número primo y G un grupo de orden p^n y $H \subset G$ un subgrupo de orden p^i. Entonces, existe un subgrupo de $H' \subseteq G$ de orden p^{i+1}, tal que $H \lhd H'$.*

8. Teorema: *Sea $p > 0$ un número primo y G un grupo de orden p^n. Entonces, G es un grupo resoluble.*

4.2.1. Resolubilidad de los grupos S_2, S_3 y S_4. Irresolubilidad de S_n, para $n > 4$

9. Definición : Se dice que un grupo G es simple cuando no contiene subgrupos normales no triviales (es decir, distintos de $\{1\}$ y G).

10. Teorema : *S_2 es un grupo abeliano simple y A_2 es trivial.*

Demostración. Inmediato, por ser $|S_2| = 2! = 2$. □

11. Definición : Una serie normal $1 \subset H_1 \subset \cdots \subset H_r = G$ se dice que es una *serie de composición* cuando sus términos son distintos y sus factores H_i/H_{i+1} son grupos simples.

12. Teorema : *S_3 es resoluble y admite una única cadena de composición:*

$$\{Id\} \subset A_3 \subset S_3$$

Es decir, A_3 es el único subgrupo normal de S_3 y es simple (abeliano).

Demostración. En efecto, $|A_3| = 3$, luego A_3 es cíclico de orden 3 y la cadena anterior es de composición. Por tanto, S_3 es resoluble. La unicidad de la cadena se obtiene de que los únicos subgrupos de orden 2 son los generados por las transposiciones y, por tanto, ninguno es normal y además los elementos de orden 3 son los 3 ciclos y cada uno de ellos genera A_3. □

13. Notación : Denotaremos $N_r = \{1, 2, \ldots, r\}$.

Sea $K_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si identificamos como conjuntos $K_4 = N_4$, entonces por el teorema de Cayley se tiene $K_4 \hookrightarrow S_4$, operando K_4 en K_4 por traslación por la derecha. Se puede observar que K_4 se identifica con el subconjunto de los pares de ciclos disjuntos

$$K_4 = \{Id, (1,2) \circ (3,4), (1,3) \circ (2,4), (1,4) \circ (2,3)\}$$

que es un subgrupo (trivialmente normal) de S_4, es decir, el subgrupo resultante es independiente de la identificación K_4 con N_4.

A este subgrupo $K_4 \subset A_4$ (normal en S_4) es al que denominaremos **grupo de Klein**.

14. Proposición : *Se verifica un isomorfismo canónico $S_4/K_4 \approx S_3$. Además, cada subgrupo $S_3 \subset S_4$ es un suplementario de K_4, es decir, $S_4 \approx K_4 \rtimes S_3$.*

Demostración. En efecto, S_3 tiene orden complementario que K_4 en S_4 y $S_3 \cap K_4 = \{Id\}$, ya que cada elemento de K_4 (salvo Id) no deja fijo ningún punto de $N_4 = K_4$ (operando por traslación). Se concluye. □

15. Corolario : *S_4 es un grupo resoluble. Es más, la siguiente cadena es de composición,*

$$\{Id\} \subset \mathbb{Z}/2\mathbb{Z} \subset K_4 \subset A_4 \subset S_4$$

Simplicidad del grupo alternado.

16. Lema : *El grupo alternado, A_n, está generado por los tres ciclos ($n > 2$).*

Demostración. Si $\sigma = (i, j, k) \in S_n$ es un tres ciclo, entonces $\operatorname{sign}(\sigma) = (-1)^2 = 1$ y $\sigma \in A_n$. Por la proposición 4.1.7, toda permutación par es producto de un número par de transposiciones. Tenemos que probar que todo producto de dos transposiciones es producto de tres ciclos. Basta observar que $(1,2)(2,3) = (1,2,3)$ (cuando las transposiciones no sean disjuntas) y $(1,2)(3,4) = (1,2,3)(2,3,4)$ (cuando las transposiciones sean disjuntas). □

17. Teorema: *Si $n \neq 4$, el único subgrupo normal propio de S_n es A_n. Los únicos subgrupos normales propios de S_4 son el alternado A_4 y el grupo de Klein K_4.*

Demostración. Por lo visto anteriormente, el teorema es claro para $n = 2, 3$, luego podemos suponer $n \geq 4$.

Por ser $H \subset S_n$ normal y el teorema 4.1.6, si $\sigma \in H$, entonces todas las permutaciones con la misma forma que σ pertenecen también a H.

Sea $Id \neq \sigma \in H$ y sea $\sigma = \sigma_1 \circ \cdots \circ \sigma_h$ su descomposición en ciclos disjuntos de órdenes respectivos $n_1 \geq \cdots \geq n_h$.

• Si $n_1 \geq 3$, digamos $\sigma_1 = (a_1, a_2, a_3, \ldots, a_{n_1})$, sea $\overline{\sigma}_1 = (a_{n_1}, \ldots, a_3, a_1, a_2)$. Se verifica que $\overline{\sigma} = \overline{\sigma}_1 \circ \sigma_2^{-1} \circ \cdots \circ \sigma_h^{-1} \in H$, pues tiene la misma forma que σ. Luego, $\overline{\sigma} \circ \sigma = (a_1, a_{n_1}, a_2) \in H$ y por el lema 4.2.16, se concluye que H contiene a A_n. Por tanto, $H = A_n$ ó S_n.

• Si $n_1 = 2$ y $h = 1$, entonces σ es una transposición y H las contiene a todas, luego $H = S_n$ (proposición 4.1.7).

• Por último, si $n_1 = 2$ y $h \geq 2$, entonces $\sigma = (a_1, a_2) \circ (a_3, a_4) \circ \sigma_3 \circ \cdots \circ \sigma_h$. Eligiendo la permutación con la misma forma $\overline{\sigma} = (a_1, a_3) \circ (a_2, a_1) \circ \sigma_3^{-1} \circ \cdots \circ \sigma_h^{-1}$, se obtiene que

$$\tau := (a_1, a_4) \circ (a_2, a_3) = \overline{\sigma} \circ \sigma \in H$$

y, por tanto H contiene a todos los pares de trasposiciones disjuntas. Si $n > 4$, sea $\tau' = (a_2, a_3) \circ (a_1, a_5)$, entonces $(a_1, a_5, a_4) = \tau \circ \tau' \in H$. Luego, H contiene a todos los tres ciclos y $A_n \subseteq H$. Entonces, $H = S_n$ ó $H = A_n$. Si $n = 4$, entonces H contiene al grupo de Klein y $H/K_4 \subset S_4/K_4 \approx S_3$ es un subgrupo normal, es decir, es trivial o A_3 y, por tanto, $H = K_4$ o A_4. □

18. Teorema: *A_n es simple para $n \neq 4$.*

Demostración. Sea $H \subset A_n$ normal no trivial. Se verifica que $N_{S_n}(H) = A_n$ (por el teorema anterior). Es decir, que H tiene exactamente dos conjugados (por S_n) uno es H y el otro es $H' = \sigma \circ H \circ \sigma^{-1}$ para cualquier permutación impar σ. En particular, $H \cap H' = \{id\}$ y $H \cdot H' = A_n$, pues ambos son subgrupos normales en S_n, es decir, $A_n \approx H \times H'$. De aquí que H tiene orden par (por tenerlo A_n) y, por tanto, contiene un elemento μ de orden 2 (teorema de Cauchy). De aquí que μ descompone en producto de trasposiciones disjuntas $\mu = \sigma_1 \circ \cdots \circ \sigma_h$. Por tanto, $\mu = \sigma_1 \circ \mu \circ \sigma_1^{-1} \in H'$, es decir, $\mu \in H \cap H' = \{Id\}$ y se obtiene una contradicción.

□

19. Corolario: *La única serie de composición de S_n, para $n > 4$, es*

$$\{Id\} \subset A_n \subset S_n$$

Demostración. $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$ y A_n es simple, luego la serie es de composición. La unicidad es consecuencia de los dos teoremas anteriores. □

4.3. Resolución de ecuaciones polinómicas por radicales

Sea $k \hookrightarrow K$ una extensión de Galois de grupo G, $\alpha \in K$ y H_α el subgrupo de isotropía de α. El polinomio mínimo anulador de α con coeficientes en k, es el polinomio

$$p(x) = \prod_{\bar{g} \in G/H_\alpha} (x - g(\alpha))$$

En efecto, consideremos la operación natural de G en $K[x]$, $g(\sum_i a_i x^i) := \sum_i g(a_i) x^i$. Por el teorema de Artin, $q(x) \in K[x]$ es invariante por G si y sólo si $q(x) \in k[x]$. Es claro que $p(x)$ es invariante por G, luego $p(x) \in k[x]$.

Además, $p(x)$ anula a α. Si α es una raíz de $q(x) \in k[x]$, entonces $g(\alpha)$ es una raíz de $g(q(x)) = q(x)$, para todo $g \in G$. Por tanto, el polinomio mínimo anulador de α es $p(x)$.

Sea $p(x) \in k[x]$ un polinomio irreducible y supongamos por sencillez que $p'(x) \neq 0$ (es decir, la extensión $k \hookrightarrow k[x]/(p(x))$ es separable). Sean $\alpha_1, \ldots, \alpha_n$ las raíces de $p(x)$, en el cierre algebraico de k y sea $k(\alpha_1, \ldots, \alpha_n)$ el cuerpo de descomposición de $p(x)$. El morfismo $k[x_1, \ldots, x_n] \to k(\alpha_1, \ldots, \alpha_n)$, $x_i \mapsto \alpha_i$ es epiyectivo, por tanto, $k(\alpha_1, \ldots, \alpha_n) = k[x_1, \ldots, x_n]/\mathfrak{m}$, donde $\mathfrak{m}$ es el ideal formado por todos los polinomios $p(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ tales que $p(\alpha_1, \ldots, \alpha_n) = 0$. Sea $G = \mathrm{Aut}_{k-alg}\, k(\alpha_1, \ldots, \alpha_n)$ el grupo de Galois de $p(x)$. Todo $\tau \in G$ aplica cada raíz $p(x)$ en otra raíz de $p(x)$ y τ queda determinado por como opera sobre los raíces de $p(x)$. En conclusión, si consideramos la acción natural de S_n en $k[x_1, \ldots, x_n]$, $\sigma(q(x_1, \ldots, x_n)) = q(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, tenemos que

$$\mathrm{Aut}_{k-alg}\, k(\alpha_1, \ldots, \alpha_n) = \{\sigma \in S_n \colon \sigma(\mathfrak{m}) = \mathfrak{m}\}$$

Es decir, el grupo de Galois de $p(x)$ es el conjunto de permutaciones σ de las raíces de $p(x)$, tales que si $q(\alpha_1, \ldots, \alpha_n) = 0$ entonces $q(x_{\sigma_1}, \ldots, x_{\sigma_n}) = 0$.

Como $p(x)$ es irreducible el grupo de Galois de $p(x)$, G, opera transitivamente sobre las raíces, es decir, G es un subgrupo transitivo [1] de S_n.

El objetivo de esta sección es probar que las raíces de $p(x)$ se pueden obtener como combinaciones algebraicas y toma de radicales sucesivas de elementos de k si y sólo si G es resoluble.

Extensiones de cuerpos cíclicas y extensiones por radicales.

1. Definición : Diremos que una extensión $k \to K$ es *cíclica* si es de Galois de grupo cíclico.

Para ver la estructura de las extensiones cíclicas necesitamos algunos conceptos y resultados previos.

Sea $k \to K$ una extensión de Galois de grupo $G = \{g_1, \ldots, g_n\}$ y sea $\alpha \in K$. Llamaremos *norma de* α, que denotaremos $N(\alpha)$, a

$$N(\alpha) := g_1(\alpha) \cdot \cdots \cdot g_n(\alpha)$$

Es claro que $N(\alpha)$ es invariante por G, luego pertenece a k. Llamaremos *traza de* α, que denotaremos $Tr(\alpha)$, a

$$Tr(\alpha) = g_1(\alpha) + \cdots + g_n(\alpha)$$

que es también invariante por G, luego pertenece a k.

2. Ejercicio : Probar que $N(g \cdot \alpha) = N(\alpha)$ y $Tr(g \cdot \alpha) = Tr(\alpha)$, para todo $\alpha \in K$ y $g \in G$.

3. Teorema (de independencia lineal de Artin): *Sea $k \to K$ una extensión de Galois de grupo $G = \{g_1, \ldots, g_n\}$. Se verifica que $g_1, \ldots, g_n$ son linealmente independientes sobre k (como endomorfismos).*

Demostración. Los automorfismos de K se corresponden, por la fórmula de los puntos, con los puntos racionales de $K \underset{k}{\otimes} K$. Ahora, como $k \to K$ es de Galois, $K \underset{k}{\otimes} K = K \times \overset{n}{\cdots} \times K$, y los automorfismos de K se corresponden con las proyecciones de $K \times \overset{n}{\cdots} \times K$ en cada uno de los factores, que son claramente linealmente independientes. □

4. Observación : La misma demostración sirve para probar que $\lambda_1 g_1, \ldots, \lambda_n g_n$, con $0 \neq \lambda_i \in K$, son linealmente independientes sobre k (se entiende que $\lambda_i g_i$ es endomorfismo por $(\lambda_i g_i)(\mu) = \lambda_i \cdot g_i(\mu)$).

5. Teorema 90 de Hilbert : *Sea $k \to K$ una extensión cíclica de grado n y grupo $G =< \sigma >$. Entonces*

$$N(\alpha) = 1 \Leftrightarrow \alpha = \frac{\beta}{\sigma(\beta)}$$

[1] Sea X un G-conjunto. Se dice que G opera transitivamente sobre X si X es una sóla órbita, es decir, para toda pareja $x, x' \in X$ existe un $g \in G$ de modo que $x' = gx$. Diremos que un subgrupo de permutaciones $G \subset S_n = Biy\{1, \ldots, n\}$ es transitivo si opera transitivamente en $\{1, \ldots, n\}$.

Demostración. Si $\alpha = \frac{\beta}{\sigma(\beta)}$, entonces

$$N(\alpha) = N\left(\frac{\beta}{\sigma(\beta)}\right) = \frac{N(\beta)}{N(\sigma(\beta))} = 1$$

Recíprocamente, supongamos que $N(\alpha) = 1$. Sea $T = \alpha\sigma$. Entonces $T^2 = \alpha\sigma(\alpha)\sigma^2$, y así sucesivamente, $T^n = \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha)\sigma^n = N(\alpha) = 1$. Por tanto, $x^n - 1$ anula a T. Es más, por el teorema de independencia lineal de Artin (y su observación posterior), $1, T, \ldots, T^{n-1}$ son linealmente independientes, luego $x^n - 1$ es el anulador de T. Como tiene la raíz 1, existe algún vector propio no nulo de valor propio 1, es decir, existe $\beta \in K$ tal que $T(\beta) = \beta$, es decir, $\alpha = \frac{\beta}{\sigma(\beta)}$. □

6. Corolario: *Sea k un cuerpo de característica $p \geq 0$, $n > 0$ no divisible por p y supongamos k contiene todas las raíces n-ésimas de la unidad. Si $k \to K$ una extensión cíclica de grado n, entonces existe $a \in k$ de modo que*

$$K = k(\sqrt[n]{a})$$

Demostración. Sea ϵ una raíz primitiva n-ésima de la unidad. Como $\epsilon \in k$, entonces $N(\epsilon) = \epsilon^n = 1$, luego por el teorema 90 de Hilbert, existe $\beta \in K$ tal que

$$\epsilon = \frac{\beta}{\sigma(\beta)}$$

siendo σ un generador del grupo de la extensión. Entonces $\sigma(\beta) = \epsilon^{-1}\beta$, luego $\sigma(\beta^n) = \epsilon^{-n}\beta^n = \beta^n$, es decir, β^n es invariante por σ, luego por todo el grupo, luego pertenece a k, $\beta^n = a \in k$. En definitiva $\beta = \sqrt[n]{a}$. Para concluir, veamos que $K = k(\sqrt[n]{a})$. Como $k(\beta)$ es una subextensión de K, será $k(\beta) = K^H$ para cuerpo subgrupo H. Además $H =< \sigma^i >$ para algún i. Luego $\beta = \sigma^i(\beta) = \epsilon^{-i}\beta$, y como ϵ es una raíz primitiva, debe ser $i = n$, es decir, $H = \{Id\}$ y por tanto $k(\beta) = K^{Id} = K$. □

7. Observación: 1) En el corolario anterior se ha probado además que $x^n - a$ es irreducible: en efecto, hemos visto que $K = k(\beta)$, luego el polinomio mínimo de β es de grado n, y por tanto es $x^n - a$, luego este es irreducible. Se dice entonces que $\sqrt[n]{a}$ es un "radical propio" (es decir, su polinomio mínimo es $x^n - a$).

2) En la demostración del corolario anterior se ha visto que $\beta = \sqrt[n]{a}$, para algún $a \in k$, si y sólo si $\sigma(\beta) = \epsilon\beta$, siendo ϵ una raíz n-ésima de la unidad. Además $\beta = \sqrt[n]{a}$ es un radical propio si y sólo si $\sigma(\beta) = \epsilon\beta$, siendo ϵ una raíz primitiva n-ésima de la unidad.

Resolvente de Lagrange.

Sea $k \to K$ una extensión cíclica de grado n, primo con la característica, supongamos que k contiene a las raíces n-ésimas de la unidad y fijemos una raíz n-ésima primitiva de la unidad, ϵ. Sea σ un generador del grupo de la extensión y $\beta \in K$, tal que $\sigma(\beta) = \epsilon \cdot \beta$, luego $a := \beta^n \in k$ y $\beta = \sqrt[n]{a}$. Sabemos que $K = k(\beta)$.

Veamos ahora cómo expresar, de modo explícito, un elemento α de una extensión cíclica $K = k(\beta)$ en función de radicales de elementos de k.

Dado $\alpha \in K$, se tiene que $\alpha = \sum_{i=0}^{n-1} c_i\beta^i$, para ciertos $c_i \in k$. Queremos calcular los c_i (como $b_i := (c_i\beta^i)^n = c_i^n a^i \in k$, es decir, $c_i\beta^i = \sqrt[n]{b_i}$, nos basta con calcular $c_i\beta^i$, para todo i). Sea $p(x) := \sum_i c_i x^i$ y $q(x) := p(\beta \cdot x)$. Observemos que

$$\begin{aligned}
&q(1) = p(\beta) = \alpha \\
&q(\epsilon) = p(\epsilon \cdot \beta) = p(\sigma(\beta)) = \sigma(p(\beta)) = \sigma(\alpha) \\
&\cdots \\
&q(\epsilon^{n-1}) = p(\epsilon^{n-1}\beta) = p(\sigma^{n-1}(\beta)) = \sigma^{n-1}(p(\beta)) = \sigma^{n-1}(\alpha)
\end{aligned}$$

Por la fórmula de interpolación de Lagrange (2.4.1),

$$q(x) = \frac{1}{n}\sum_{i=0}^{n-1} \frac{x^n - 1}{x - \epsilon^i}\epsilon^i\sigma^i(\alpha)$$

Un sencillo cálculo, muestra que el coeficiente j-ésimo de este polinomio es igual a

$$c_j\beta^j = \frac{1}{n}(\alpha + \epsilon^{-j}\sigma(\alpha) + \cdots + \epsilon^{-(n-1)j}\sigma^{n-1}(\alpha)) = \frac{1}{n}\sum_{i=0}^{n-1}(\epsilon^{-j})^i\sigma^i(\alpha) =: \frac{1}{n}R(\alpha, \epsilon^j)$$

Por tanto, como $\alpha = \sum_{j=0}^{n-1} c_j\beta^j$,

$$\boxed{\alpha = \frac{1}{n}\sum_{j=0}^{n-1} R(\alpha, \epsilon^j)}$$

8. Definición : Dado $\alpha \in K$, llamaremos resolvente de Lagrange de α por ϵ^j, que denotaremos $R(\alpha, \epsilon^j)$, a

$$R(\alpha, \epsilon^j) := \sum_{i=0}^{n-1}(\epsilon^{-j})^i\sigma^i(\alpha)$$

Este teorema se generaliza de forma sencilla al caso en el que el grupo es producto directo de grupos abelianos.

9. Teorema : *Sea K una extensión de Galois de grupo $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ ($n = n_1 \cdots n_r$ primo con la característica). Sean $\sigma_1, \ldots \sigma_r$ generadores de G de órdenes $n_1, \ldots, n_r$, respectivamente, y $\varepsilon_1, \ldots, \varepsilon_r$ raíces primitivas $n_1, \ldots, n_r$-ésimas de la unidad. Dado $\alpha \in K$, denotemos*

$$R(\alpha, \varepsilon_1^{j_1}, \ldots, \varepsilon_r^{j_r}) = \sum_{i_1 < n_1, \ldots, i_r < n_r} \varepsilon_1^{-i_1 j_1} \cdots \varepsilon_r^{-i_r j_r}\,(\sigma_1^{i_1} \circ \cdots \circ \sigma_r^{i_r})(\alpha)$$

$R(\alpha, \varepsilon_1^{j_1}, \ldots, \varepsilon_r^{j_r})$ son radicales d-ésimos (d el mínimo común múltiplo de $n_1, \ldots, n_r$) y se verifica la fórmula:

$$\alpha = \frac{1}{n}\sum_{j_1 < n_1, \ldots, j_r < n_r} R(\alpha, \varepsilon_1^{j_1}, \ldots, \varepsilon_r^{j_r})$$

Resolución de las ecuaciones por radicales.

10. Definición : Diremos que una extensión de Galois $k \to K$ es *radical* si $K \simeq k(\sqrt[n]{a})$ (suponemos que el radical es propio).

11. Definición : Diremos que una extensión $k \to K$ es *resoluble por radicales* si admite una cadena de subextensiones

$$k \to K_1 \to K_2 \to \cdots \to K_r = K$$

tal que $K_i \to K_{i+1}$ es radical. Análogamente, diremos que una ecuación, $p(x) = 0$, es resoluble por radicales si el cuerpo de descomposición de $p(x)$ es resoluble por radicales.

12. Teorema : *Sea $k \to K$ una extensión de Galois de grupo G. Entonces $k \to K$ es resoluble por radicales si y sólo si el grupo G es resoluble. (Suponemos que el cuerpo base contiene a las raíces de la unidad que hagan falta).*

Demostración. Es inmediato del teorema (clásico) de Galois y del teorema de caracterización de las extensiones cíclicas (Corolario del teorema 90 de Hilbert). □

4.3.1. Irresolubilidad de la ecuación genérica de grado $n > 4$. Resolución de las ecuaciones de grado 2,3 y 4

Sea k un cuerpo y $a_1, \ldots, a_n$ variables libres. Consideremos el cuerpo $k(a_1, \ldots, a_n)$, y el polinomio con coeficientes en este cuerpo:

$$x^n + a_1 x^{n-1} + \cdots + a_n$$

que se denomina *ecuación general de grado n sobre k*. Denotemos $\alpha_1, \ldots, \alpha_n$ a las raíces de este polinomio (que también son variables libres sobre k). El grupo simétrico de n letras, S_n, opera en $k(\alpha_1, \ldots, \alpha_n)$ de modo natural (por automorfismos de k-álgebras), permutando las α_i. Por el teorema fundamental de las funciones simétricas se obtiene que

$$k(\alpha_1, \ldots, \alpha_n)^{S_n} = k(a_1, \ldots, a_n)$$

y por el teorema de Artin se concluye que

$$k(a_1, \ldots, a_n) \to k(\alpha_1, \ldots, \alpha_n)$$

es una extensión de Galois de grupo S_n. Es decir, *el grupo de la ecuación general de grado n es* S_n.

13. Teorema : *La ecuación general de grado n es resoluble por radicales para* $n \leq 4$ *y no es resoluble por radicales para* $n > 4$.

Demostración. Se deduce de que el grupo simétrico S_n es resoluble si y sólo si $n \leq 4$. □

14. Observación : La hipótesis de que el cuerpo base contenga a la raíces n-ésimas de la unidad es innecesaria y la hemos puesto por simplificar la demostración (es decir, para poder aplicar el corolario del Teorema 90 de Hilbert multiplicativo). De hecho las raíces de la unidad son siempre resolubles por radicales propios (pruébese), y por ello puede suponerse que el cuerpo base las contiene.

15. Ejemplo : Resolución de la ecuación de segundo grado.

Sea $x^2 + ax + b$ la ecuación general de segundo grado, de raíces α_1, α_2. Como ya sabemos, el grupo de la ecuación es $S_2 = \mathbb{Z}/2\mathbb{Z}$, generado por la permutación $\sigma = (1, 2)$, $\sigma(\alpha_1) = \alpha_2$.

Calculamos las resolventes de Lagrange. Tenemos

$$R(\alpha_1, 1) = \frac{\alpha_1 + \alpha_2}{2} = -\frac{a}{2}$$
$$R(\alpha_1, -1) = \frac{\alpha_1 - \alpha_2}{2}$$

y $R(\alpha_1, -1)^2 = \frac{(\alpha_1 - \alpha_2)^2}{4} = \frac{(\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2}{4} = \frac{a^2 - 4b}{4}$. Por tanto,

$$\alpha_1, \alpha_2 = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

16. Ejemplo : Resolución de la cúbica, $x^3 + a_1 x^2 + a_2 x + a_3 = 0$**.**

Se verifica que S_3 es un grupo resoluble: el alternado $A_3 =< (1, 2, 3) >\approx \mathbb{Z}/3\mathbb{Z}$ es un subgrupo normal y $S_3/A_3 =< \overline{(1, 2)} >\approx \mathbb{Z}/2\mathbb{Z}$.

Notación: En lo que sigue, denotaremos $\sigma = (1, 2, 3)$ y $\tau = (1, 2)$.

La extensión $k \subset K^{A_3}$ es de Galois de grado 2 de grupo $S_3/A_3 =< \overline{(1, 2)} >\approx \mathbb{Z}/2\mathbb{Z}$, es decir, generado por la permutación τ y la extensión $K^{A_3} \subset K$ es de Galois de grado 3 y grupo $A_3 =< \sigma >\approx \mathbb{Z}/3\mathbb{Z}$.

Se verifica que el polinomio $\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ es un elemento estable por S_3 sobre el que opera multiplicando por el signo de la permutación, es decir, $s(\delta) = sig\,(s) \cdot \delta$, en particular es invariante por A_3 y $\Delta = \delta^2$ es invariante y como función de los coeficientes de la cúbica es:

$$\Delta = a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2 \qquad \delta = \sqrt{a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2}$$

Obviamente, $k[\delta] = K^{A_3}$.

Por la fórmula de Lagrange, las raíces $x_1, x_2, x_3 \in K$ se expresan en función de radicales cúbicos de elementos de K^{A_3} de la siguiente forma:

$$x_i = \frac{1}{3}(R(x_i, 1) + R(x_i, \varepsilon) + R(x_i, \varepsilon^2))$$

donde

$$\begin{aligned} R(x_i, 1) &= x_i + \sigma(x_i) + \sigma^2(x_i) = x_1 + x_2 + x_3 = -a_1 \\ R(x_i, \varepsilon) &= x_i + \sigma(x_i)\varepsilon^2 + \sigma^2(x_i)\varepsilon = \varepsilon^{i-1}R(x_1, \varepsilon) \\ R(x_i, \varepsilon^2) &= x_i + \sigma(x_i)\varepsilon + \sigma^2(x_i)\varepsilon^2 = \varepsilon^{2(i-1)}R(x_1, \varepsilon^2) \end{aligned}$$

Luego basta calcular los radicales cúbicos $R(x_1, \varepsilon)$ y $R(x_1, \varepsilon^2)$. Por otro lado estos dos radicales son interdependientes pues si los denotamos respectivamente R_1 y R_2 se verifica que $\sigma(R_1) = \varepsilon \cdot R_1$ y $\sigma(R_2) = \varepsilon^2 \cdot R_2$, luego $R_1 \cdot R_2$ es un invariante por A_3, es decir, $R_1 \cdot R_2 = \lambda \in K^{A_3}$ y por tanto,

$$R_2 = \frac{\lambda}{R_1}$$

Luego, basta calcular R_1^3 y $\lambda = R_1 \cdot R_2$ en función de δ. Un calculo sencillo prueba que

$$\lambda = R_1 \cdot R_2 = a_1^2 - 3a_2.$$

Por otro lado, aplicando la resolvente de Lagrange en el caso de $q = 2$, se obtiene:

$$R_1^3 = \frac{1}{2}(R_1^3 + \tau(R_1^3)) + \frac{1}{2}(R_1^3 - \tau(R_1^3))$$

Calculando resulta:

$$\begin{aligned} \frac{1}{2}(R_1^3 + \tau(R_1^3)) &= \frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} \\ \frac{1}{2}(R_1^3 - \tau(R_1^3)) &= \frac{3}{2}\sqrt{-3\Delta} \end{aligned}$$

Observación: Como se puede comprobar es $\tau(R_1) = \varepsilon^2 R_2$, luego $\tau(R_1^3) = R_2^3$. Por lo tanto, $R_2^3 = \frac{1}{2}(R_1^3 + \tau(R_1^3)) - \frac{1}{2}(R_1^3 - \tau(R_1^3))$.

En conclusión, resulta:

$$\boxed{\begin{aligned} x_i = \frac{1}{3}\Big(-a_1 + \sqrt[3]{\frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} + \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}} + \\ \sqrt[3]{\frac{-2a_1^3 + 9a_1a_2 - 27a_3}{2} - \frac{3}{2}\sqrt{-3(a_1^2a_2^2 - 4a_1^3a_3 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2)}}\ \Big) \end{aligned}}$$

donde los dos radicales cúbicos no son independientes, ya que, como dijimos, el primero determina el segundo pues el producto de estos dos es $R_1 \cdot R_2 = a_1^2 - 3a_2$.

17. Ejemplo : Resolución de la cuártica, $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0$**.**

S_4 es un grupo resoluble: se tiene la cadena normal $K_4 \subset A_4 \subset S_4$ donde

$$K_4 =< (1,2)(3,4), (1,3)(2,4) >\approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

es el grupo de Klein y los factores son $A_4/K_4 =< \overline{(1,2,3)} >\approx \mathbb{Z}/3$ y $S_4/A_4 =< \overline{(1,2)} >\approx \mathbb{Z}/2\mathbb{Z}$.

Notación: Denotaremos $s_1 = (1,2)(3,4)$ y $s_2 = (1,3)(2,4)$.

La extensión $K^{K_4} \subset K$ es de Galois de grado 4 y de grupo $K_4 \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, generado por las permutaciones s_1, s_2.

Sean

$$\theta_1 = x_1x_2 + x_3x_4$$
$$\theta_2 = x_1x_3 + x_2x_4$$
$$\theta_3 = x_1x_4 + x_2x_3$$

Se verifica que una permutación τ deja fijos a estos 3 elementos si y sólo si $\tau \in K_4$, luego $K^{K_4} = k(\theta_1, \theta_2, \theta_3)$. Además el grupo simétrico permuta estos elementos entre sí (dando una identificación de S_4/K_4 con S_3) y, por tanto, son las raíces de una cúbica con coeficientes en k, a saber:

$$(x-\theta_1)(x-\theta_2)(x-\theta_3) = x^3 + a_2x^2 + (a_1a_3 - 4a_2)x - (a_1^2a_4 - 4a_2a_4 + a_3^2)$$

Esta cúbica es a la que se denomina *cúbica resolvente*.

Apliquemos la fórmula de Lagrange generalizada al caso no cíclico (como es K_4).

Las resolventes de x_1 respecto de $K_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ son:

$$R(x_1, 1, 1) = x_1 + x_2 + x_3 + x_4 = -a_1$$
$$R(x_1, -1, 1) = x_1 - x_2 + x_3 - x_4 = \xi_1$$
$$R(x_1, 1, -1) = x_1 + x_2 - x_3 - x_4 = \xi_2$$
$$R(x_1, -1, -1) = x_1 - x_2 - x_3 + x_4 = \xi_3$$

donde ξ_1, ξ_2, ξ_3 son radicales cuadráticos sobre $K^{K_4} = k(\theta_1, \theta_2, \theta_3)$, es decir, $\xi_1^2, \xi_2^2, \xi_3^2 \in K^{K_4}$ y verifican la relación $\xi_1\xi_2\xi_3 = -a_1^3 + 4a_1a_2 - 8a_3$. Como se puede comprobar es: $\xi_i^2 = a_1^2 - 4a_2 + 4\theta_i$, luego $K^{K_4} = k(\xi_1^2, \xi_2^2, \xi_3^2)$.

Resolviendo la cúbica resolvente se concluye, por ser:

$$\boxed{x_i = \frac{1}{4}(-a_1 + \sqrt{a_1^2 - 4a_2 + 4\theta_1} + \sqrt{a_1^2 - 4a_2 + 4\theta_2} + \sqrt{a_1^2 - 4a_2 + 4\theta_3})}$$

donde el producto de cada dos de estos radicales cuadráticos determinan el tercero, pues el producto de los tres es $-a_1^3 + 4a_1a_2 - 8a_3$.

4.4. Extensiones cuadráticas

Sea k un cuerpo, de característica distinta de dos.

Dado $a \in k$, la extensión $k \hookrightarrow k(\sqrt{a})$ tiene grado 1 o 2 según que $\sqrt{a}$ pertenezca a k o no. Recíprocamente, si $k \hookrightarrow K$ es una extensión de grado 2, entonces $K = k(\alpha)$, donde α es una raíz de un polinomio con coeficientes en k, irreducible de grado 2. La bien conocida fórmula de las raíces de los polinomios de grado 2, prueba que $K = k(\sqrt{a})$, para cierto $a \in k$.

1. Definición : Diremos que una extensión finita de cuerpos $k \hookrightarrow K$ es una extensión por radicales cuadráticos si $K = k(\alpha_1, \ldots, \alpha_n)$, donde $\alpha_i^2 \in k(\alpha_1, \ldots, \alpha_{i-1})$, para todo $1 \leq i \leq n$.

De la discusión anterior se sigue que el grado de extensión por radicales cuadráticos es una potencia de 2. Además, es obvio que el compuesto de un número finito de extensiones por radicales cuadráticos de k es una extensión por radicales cuadráticos de k.

2. Teorema: *Sea $k \hookrightarrow K$ una extensión de Galois. K es una extensión por radicales cuadráticos de k si y sólo si es de grado una potencia de* 2*.*

Demostración. Sólo tenemos que probar el recíproco. Como $\#G = 2^n$, entonces G es resoluble y existe una serie normal $\{1\} \subset G_1 \subset \cdots \subset G_n = G$ de factores isomorfos a $\mathbb{Z}/2\mathbb{Z}$. Esta sucesión de grupos por toma de invariantes se corresponde con una sucesión de subcuerpos $K \supset K^{G_1} \supset \cdots \supset K^{G_n} = k$, cada uno de grado 2 sobre el anterior. Por tanto, $K^{G_i} = K^{G_{i-1}}(\alpha_i)$, donde b$\alpha_i^2 \in K^{G_i}$. Luego, $K = k(\alpha_1, \ldots, \alpha_n)$ es una extensión por radicales cuadráticos. □

3. Ejercicio: Sea $K = k(x_1, \ldots, x_4)$ el cuerpo descomposición de la ecuación genérica de grado 4. Sea $H = \langle(1, 2, 3)\rangle \subset S_4$. Probar que el grado de la k-extensión K^H es 2^3 y que la envolvente de Galois de K^H es K que es de grado 24. Probar que K^H no es una extensión por radicales cuadráticos.

4. Definición: Diremos que un elemento $\alpha \in K$ de una extensión de cuerpos de k es un irracional cuadrático de k, si existe una extensión por radicales cuadráticos de k que contiene a α. Diremos que un polinomio con coeficientes en k es resoluble por radicales cuadráticos si todas sus raíces son irracionales cuadráticos.

Si un polinomio es irreducible y una raíz es un irracional cuadrático entonces todas las raíces son irracionales cuadráticos, ya que si α y β son raíces de $p(x)$, entonces $k(\alpha) = k[x]/(p(x)) = k(\beta)$.

5. Teorema: *Un polinomio irreducible con coeficientes en k es resoluble por irracionales cuadráticos si y sólo si es separable y su grupo de Galois es un grupo de orden una potencia de* 2*.*

Demostración. Si el polinomio es resoluble por irracionales cuadráticos entonces su cuerpo de descomposición puede incluirse en una extensión por radicales cuadráticos de k, luego es separable y es de Galois. Por tanto, el cuerpo de descomposición de $p(x)$ es de grado una potencia de 2, luego su grupo de Galois es un grupo de orden una potencia de 2.

Si el polinomio es separable y su grupo de Galois es un grupo de orden una potencia de 2, entonces su cuerpo de descomposición es una extensión por radicales cuadráticos de k y las raíces del polinomio son irracionales cuadráticos.

□

6. Ejercicio: Si α es un irracional cuadrático sobre k, pruébese que $k(\alpha)$ es una extensión de k por radicales cuadráticos.

4.5. Construcciones con regla y compás

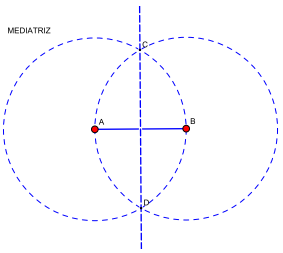
Consideremos en el plano euclídeo un conjunto de puntos $\mathbb{P}$, de cardinal mayor o igual que dos. El conjunto $C(\mathbb{P})$ de los puntos del plano euclídeo constructibles con regla y compás a partir de $\mathbb{P}$ se define inductivamente mediante la aplicación reiterada de un número finito de las siguientes construcciones:

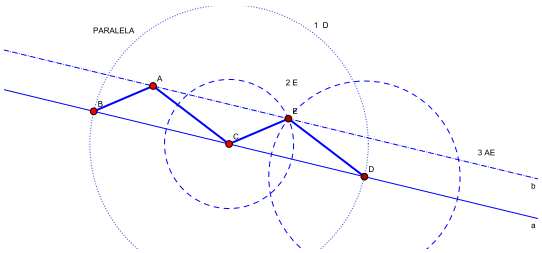
1. Los puntos de $\mathbb{P}$ son constructibles.
2. Diremos que las rectas que pasan por un par de puntos constructibles son constructibles.
3. Diremos que las circunferencias de centro un punto constructible y radio la distancia entre dos puntos constructibles son constructibles.

4. Los puntos de corte entre dos líneas constructibles (rectas o circunferencias) son constructibles.

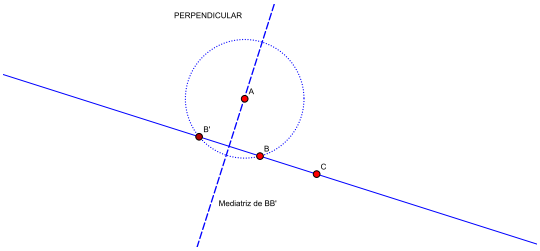
5. $C(\mathbb{P})$ es el conjunto de todos los puntos constructibles (con regla y compás a partir de $\mathbb{P}$).

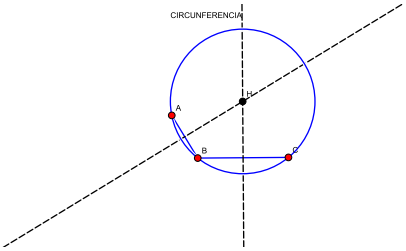
Es bien conocido que las siguiente construcciones pueden realizarse con regla y compás:
- Trazar la perpendicular por su punto medio a un segmento dado.
- Dados tres puntos no alineados A, B, C, trazar la paralela a la recta BC que pasa por A.



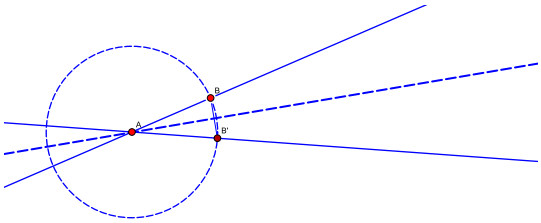


- Dados tres puntos no alineados A, B, C, trazar la perpendicular a la recta BC que pasa por A.
- Trazar la circunferencia que pasa por tres puntos no alineados A, B y C





- Trazar la bisectriz de un ángulo dado.



Escojamos dos puntos de $\mathbb{P}$ como sistema de referencia, uno el origen de coordenadas $(0,0)$ y el otro el $(0,1)$. Identifiquemos el plano euclídeo con $\mathbb{C}$. Los puntos escogidos se corresponden con el 0 y 1 de $\mathbb{C}$. Los puntos de $\mathbb{C}(\mathbb{P})$ se corresponden con ciertos números complejos. A partir de ahora identificamos los puntos del plano euclídeo con los correspondientes números complejos.

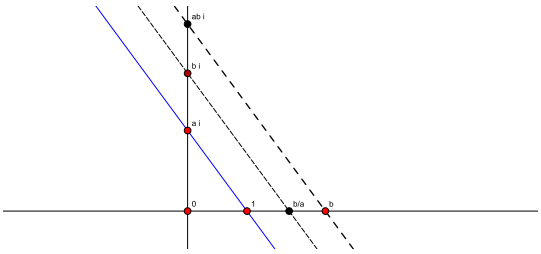
1. Lema: *La condición necesaria y suficiente para que un número complejo $a + bi$ sea constructible es que lo sean su parte real a y su parte imaginaria b.*

Demostración. Es consecuencia directa de la posibilidad de trazar paralelas y perpendiculares con regla y compás. □

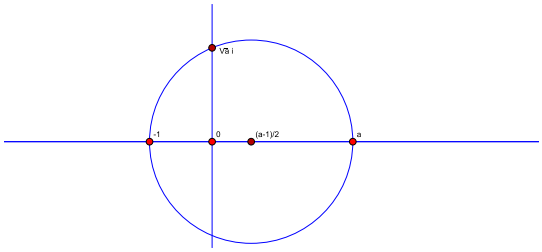
2. Lema: *Los números complejos constructibles $C(\mathbb{P})$, forman un subcuerpo de $\mathbb{C}$, estable por toma de raíces cuadradas.*

Demostración. La suma y diferencia de dos números complejos constructibles es constructible: Por el lema anterior, podemos suponer que los dos números dados son reales y este caso es trivial.

El producto y cociente de dos números complejos constructibles es constructible: Por el lema anterior, podemos suponer que los dos números dados son reales. En la siguiente figura construimos el producto y cociente de a y b.



Para concluir hay que demostrar que la raíz cuadrada de cualquier número complejo constructible también lo es. Si el número es real, basta considerar la siguiente figura:



En el caso de un número complejo arbitrario, se construye la bisectriz del ángulo que determina con el 1 y se traza en ella el segmento de longitud igual a la raíz cuadrada del módulo del número complejo dado.

□

3. Teorema: *Sea k el mínimo subcuerpo de $\mathbb{C}$ que contiene a $\mathbb{P}$. La condición necesaria y suficiente para que un número complejo sea constructible a partir de $\mathbb{P}$ es que sea un irracional cuadrático de k.*

Demostración. Si α es constructible, entonces $k(\alpha)$ es una extensión de k por radicales cuadráticos. Por el lema anterior, α es constructible.

Para demostrar el recíproco, obsérvese que los coeficientes de las ecuaciones de las rectas y circunferencias son funciones racionales de las coordenadas de los puntos que las determinan, según las construcciones 2 y 3. Además, las coordenadas de la intersección de dos líneas (círculos o rectas), se expresan en función de los coeficientes de las ecuaciones como irracionales cuadráticos. Procediendo inductivamente concluimos que las coordenadas de cualquier punto constructible son irracionales cuadráticos sobre k. Es decir, si $a + bi$ es constructible, es un irracional cuadrático sobre k.

□

4.6. Biografía de Abel

ABEL BIOGRAPHY

Niels Abel's life was dominated by poverty and we begin by putting this in context by looking briefly at the political problems which led to economic problems in Norway. At the end of the 18th century Norway was part of Denmark and the Danish tried to remain neutral through the Napoleonic wars. However a neutrality treaty in 1794 was considered a aggressive act by Britain and, in 1801, the British fleet destroyed most of the Danish fleet in a battle in the harbour at Copenhagen. Despite this Denmark-Norway avoided wars until 1807 when Britain feared that the Danish fleet might be used by the French to invade. Using the philosophy that attack is the best form of defence, the English attacked and captured the whole Danish fleet in October 1807.

Denmark then joined the alliance Britain Britain. The continental powers blockaded Britain, and as a counter to this Britain blockaded Norway. The twin blockade was a catastrophe to Norway preventing their timber exports, which had been largely to Britain, and preventing their grain imports from Denmark. An economic crisis in Norway followed with the people suffering hunger and extreme poverty. In 1813 Sweden attacked Denmark from the south and, at the treaty of Kiel in January 1814, Denmark handed over Norway to Sweden. An attempt at independence by Norway a few months later led to Sweden attacking Norway in July 1814. Sweden gained control of Norway, setting up a complete internal self-government for Norway with a government in Christiania (which is called Oslo today). In this difficult time Abel was growing up in Gjerstad in south-east Norway.

Abel's father, Sören Georg Abel, had a degree in theology and philology and his father (Niels Abel's grandfather) was a Protestant minister at Gjerstad near Risor. Sören Abel was a Norwegian nationalist who was active politically in the movement to make Norway independent. Sören Abel married Ane Marie Simonson, the daughter of a merchant and ship owner, and was appointed as minister at Finnoy. Niels Abel, the second of seven children, was one year old when his grandfather died and his father was appointed to succeed him as the minister at Gjerstad. It was in that town that Abel was brought up, taught by his father in the vicarage until he reached 13 years of age. However, these were the 13 years of economic crisis for Norway described above and Abel's parents would have not been able to feed their family that well. The problems were not entirely political either for

[Abel's] father was probably a drunkard and his mother was accused of having lax morals.

Abel's father was, however, important in the politics of Norway and, after Sweden gained control of Norway in 1814, he was involved in writing a new constitution for Norway as a member of the Storting, the Norwegian legislative body. In 1815 Abel and his older brother were sent to the Cathedral School in Christiania. The founding of the University of Christiania had taken away the good teachers from the Cathedral School to staff the University when it opened for teaching in 1813. What had been a good school was in a bad state when Abel arrived. Uninspired by the poor school, he proved a rather ordinary pupil with some talent for mathematics and physics.

When a new mathematics teacher Bernt Holmboë joined the school in 1817 things changed markedly for Abel. The previous mathematics teacher had been dismissed for punishing a boy so severely that he had died. Abel began to study university level mathematics texts and, within a year of Holmboë's arrival, Abel was reading the works of Euler, Newton, Lalande and d'Alembert. Holmboë was convinced that Abel had great talent and encouraged him greatly taking him on to study the works of Lagrange and Laplace. However, in 1820 tragedy struck Abel's family when his father died.

Abel's father had ended his political career in disgrace by making false charges against his colleagues in

the Storting after he was elected to the body again in 1818. His habits of drinking to excess also contributed to his dismissal and the family was therefore in the deepest trouble when he died. There was now no money to allow Abel to complete his school education, nor money to allow him to study at university and, in addition, Abel had the responsibility of supporting his mother and family.

Holmboë was able to help Abel gain a scholarship to remain at school and Abel was able to enter the University of Christiania in 1821, ten years after the university was founded. Holmboë had raised money from his colleagues to enable Abel to study at the university and he graduated in 1822. While in his final year at school, however, Abel had begun working on the solution of quintic equations by radicals. He believed that he had solved the quintic in 1821 and submitted a paper to the Danish mathematician Ferdinand Degen, for publication by the Royal Society of Copenhagen. Degen asked Abel to give a numerical example of his method and, while trying to provide an example, Abel discovered the mistake in his paper. Degen had given Abel some important advice that was to set him working on an area of mathematics,

... whose development would have the greatest consequences for analysis and mechanics. I refer to elliptic integrals. A serious investigator with suitable qualifications for research of this kind would by no means be restricted to the many beautiful properties of these most remarkable functions, but could discover a Strait of Magellan leading into wide expanses of a tremendous analytic ocean.

At the University of Christiania Abel found a supporter in the professor of astronomy Christopher Hansteen, who provided both financial support and encouragement. Hansteen's wife began to care for Abel as if he was her own son. In 1823 Abel published papers on functional equations and integrals in a new scientific journal started up by Hansteen. In Abel's third paper, Solutions of some problems by means of definite integrals he gave the first solution of an integral equation.

Abel was given a small grant to visit Degen and other mathematicians in Copenhagen. While there he met Christine Kemp who shortly afterwards became his fiancée. Returning to Christiania, Abel tried to get the University of Christiania to give him a larger grant to enable him to visit the top mathematicians in Germany and France. He did not speak French of German so, partly to save money, he was given funds to remain in Christiania for two years to give him the chance to become fluent in these languages before travelling. Abel began working again on quintic equations and, in 1824, he proved the impossibility of solving the general equation of the fifth degree in radicals. He published the work in French and at his own expense since he wanted an impressive piece of work to take with him when he was on his travels. As Ayoub writes

He chose a pamphlet as the quickest way to get it into print, and in order to save on the printing costs, he reduced the proof to fit on half a folio sheet [six pages].

By this time Abel seems to have known something of Ruffini's work for he had studied Cauchy's work of 1815 while he was an undergraduate and in this paper there is a reference to Ruffini's work. Abel's 1824 paper begins

Geometers have occupied themselves a great deal with the general solution of algebraic equations and several among them have sought to prove the impossibility. But, if I am not mistaken, they have not succeeded up to the present.

Abel sent this pamphlet to several mathematicians including Gauss, who he intended to visit in Göttingen while on his travels. In August 1825 Abel was given a scholarship from the Norwegian government to allow him to travel abroad and, after taking a month to settle his affairs, he set out for the Continent with four friends, first visiting mathematicians in Norway and Denmark. On reaching Copenhagen, Abel found that Degen had died and he changed his mind about taking Hansteen's advice to go directly to Paris, preferring not to travel alone and stay with his friends who were going to Berlin. As he wrote in a later letter

Now I am so constituted that I cannot endure solitude. Alone, I am depressed, I get cantankerous, and I have little inclination to work.

In Copenhagen Abel was given a letter of introduction to Crelle by one of the mathematicians there. Abel met Crelle in Berlin and the two became firm friends. This proved the most useful part of Abel's whole trip, particularly as Crelle was about to begin publishing a journal devoted to mathematical research. Abel was encouraged by Crelle to write a clearer version of his work on the insolubility of the quintic and this resulted in Recherches sur les fonctions elliptiques which was published in 1827 in the first volume of Crelle's Journal, along with six other papers by Abel. While in Berlin, Abel learnt that the position of professor of mathematics at the University of Christiania, the only university in Norway, had been given to Holmboë. With no prospects of a university post in Norway, Abel began to worry about his future.

Crelle's Journal continued to be a source for Abel's papers and Abel began to work to establish mathematical analysis on a rigorous basis. He wrote to Holmboë from Berlin:

My eyes have been opened in the most surprising manner. If you disregard the very simplest cases, there is in all of mathematics not a single infinite series whose sum had been rigorously determined. In other words, the most important parts of mathematics stand without foundation. It is true that most of it is valid, but that is very surprising. I struggle to find a reason for it, an exceedingly interesting problem.

It had been Abel's intention to travel with Crelle to Paris and to visit Gauss in Göttingen on the way. However, news got back to Abel that Gauss was not pleased to receive his work on the insolubility of the quintic, so Abel decided that he would be better not to go to Göttingen. It is uncertain why Gauss took this attitude towards Abel's work since he certainly never read it - the paper was found unopened after Gauss's death. Ayoub gives two possible reasons:

... the first possibility is that Gauss had proved the result himself and was willing to let Abel take the credit. ... The other explanation is that he did not attach very much importance to solvability by radicals...

The second of these explanations does seem the more likely, especially since Gauss had written in his thesis of 1801 that the algebraic solution of an equation was no better than devising a symbol for the root of the equation and then saying that the equation had a root equal to the symbol.

Crelle was detained in Berlin and could not travel with Abel to Paris. Abel therefore did not go directly to Paris, but chose to travel again with his Norwegian friends to northern Italy before crossing the Alps to France. In Paris Abel was disappointed to find there was little interest in his work. He wrote back to Holmboë:

The French are much more reserved with strangers than the Germans. It is extremely difficult to gain their intimacy, and I do not dare to urge my pretensions as far as that; finally every beginner had a great deal of difficulty getting noticed here. I have just finished an extensive treatise on a certain class of transcendental functions to present it to the Institute which will be done next Monday. I showed it to Mr Cauchy, but he scarcely deigned to glance at it.

The contents and importance of this treatise by Abel is described,

It dealt with the sum of integrals of a given algebraic function. Abel's theorem states that any such sum can be expressed as a fixed number p of these integrals, with integration arguments that are algebraic functions of the original arguments. The minimal number p is the genus of the algebraic function, and this is the first occurrence of this fundamental quantity. Abel's theorem is a vast generalisation of Euler's relation for elliptic integrals.

Two referees, Cauchy and Legendre, were appointed to referee the paper and Abel remained in Paris for a few months,

... emaciated, gloomy, weary and constantly worried. He ... could only afford to eat one meal a day.

He published some articles, mainly on the results he had already written for Crelle's Journal, then with no money left and his health in a very poor state, he returned to Berlin at the end of 1826. In Berlin, Abel borrowed some money and continued working on elliptic functions. He wrote a paper in which

... he radically transformed the theory of elliptic integrals to the theory of elliptic functions by using their inverse functions ...

Crelle tried to persuade Abel to remain in Berlin until he could find an academic post for him and he even offered Abel the editorship of Crelle's Journal. However, Abel wanted to get home and by this time he was heavily in debt. He reached Christiania in May 1827 and was awarded a small amount of money by the university although they made sure they had the right to deduct a corresponding amount from any future salary he earned. To make a little more money Abel tutored schoolchildren and his fiancée was employed as a governess to friends of Abel's family in Froland.

Hansteen received a major grant to investigate the Earth's magnetic field in Siberia and a replacement was needed to teach for him at the University and also at the Military Academy. Abel was appointed to this post which improved his position a little.

In 1828 Abel was shown a paper by Jacobi on transformations of elliptic integrals. Abel quickly showed that Jacobi's results were consequences of his own and added a note to this effect to the second part of his major work on elliptic functions. He had been working again on the algebraic solution of equations, with the aim of solving the problem of which equations were soluble by radicals (the problem which Galois solved a few years later). He put this to one side to compete with Jacobi in the theory of elliptic functions, quickly writing several papers on the topic.

Legendre saw the new ideas in the papers which Abel and Jacobi were writing and said

Through these works you two will be placed in the class of the foremost analysts of our times.

Abel continued to pour out high quality mathematics as his health continued to deteriorate. He spent the summer vacation of 1828 with his fiancée in Froland. The masterpiece which he had submitted to the Paris Academy seemed to have been lost and so he wrote the main result down again

The paper was only two brief pages, but of all his many works perhaps the most poignant. He called it only .^A theorem": it had no introduction, contained no superfluous remarks, no applications. It was a monument resplendent in its simple lines - the main theorem from his Paris memoir, formulated in few words.

Abel travelled by sled to visit his fiancée again in Froland for Christmas 1828. He became seriously ill on the sled journey and despite an improvement which allowed them to enjoy Christmas, he soon became very seriously ill again. Crelle was told and he redoubled his efforts to obtain an appointment for Abel in Berlin. He succeeded and wrote to Abel on the 8 April 1829 to tell him the good news. It was too late, Abel had already died. Ore [3] describes his last few days:

... the weakness and cough increased and he could remain out of bed only the few minutes while it was being made. Occasionally he would attempt to work on his mathematics, but he could no longer write. Sometimes he lived in the past, talking about his poverty and about Fru Hansteen's goodness. Always he was kind and patient. ...

He endured his worst agony during the night of April 5. Towards morning he became more quiet and in the forenoon, at eleven o'clock, he expired his last sigh.

After Abel's death his Paris memoir was found by Cauchy in 1830 after much searching. It was printed in 1841 but rather remarkably vanished again and was not found until 1952 when it turned up in Florence. Also after Abel's death unpublished work on the algebraic solution of equations was found. In fact in a letter Abel had written to Crelle on 18 October 1828 he gave the theorem:

If every three roots of an irreducible equation of prime degree are related to one another in such a way that one of them may be expressed rationally in terms of the other two, then the equation is soluble in radicals.

This result is essentially identical to one given by Galois in his famous memoir of 1830. In this same year 1830 the Paris Academy awarded Abel and Jacobi the Grand Prix for their outstanding work.

Article by: J J O'Connor and E F Robertson (http://www-history.mcs.st-and.ac.uk/Biographies/)

4.7. Problemas

1. Determinar el grupo de Galois de la cúbica $x^3 + 2x + 1$ sobre el cuerpo $\mathbb{Q}(e^{2\pi i/7})$.

2. El grupo de Galois sobre $\mathbb{Q}$ de una ecuación bicuadrada irreducible $x^4 + ax^2 + b$ es

   a) El grupo de Klein V si b es un cuadrado.

   b) El grupo cíclico C_4 si b no es un cuadrado, pero $a^2b - 4b^2$ sí lo es.

   c) El grupo diédrico D_8 en cualquier otro caso.

3. Sea α una raíz de una cuártica irreducible $p(x) \in \mathbb{Q}[x]$. Demostrar que no existen cuerpos intermedios propios entre $\mathbb{Q}$ y $\mathbb{Q}(\alpha)$ si y sólo si el grupo de Galois de $p(x)$ es el grupo simétrico S_4 o el grupo alternado A_4.

4. Si una cuártica irreducible tiene exactamente dos raíces reales, probar que su grupo de Galois sobre $\mathbb{Q}$ es el grupo simétrico S_4 o el diédrico D_8.

5. El grupo de Galois sobre $\mathbb{Q}$ de una recíproca irreducible $x^4 + ax^3 + bx^2 + ax + 1$ es

   a) El grupo de Klein V si $b^2 + 4b + 4 - 4a^2$ es un cuadrado.

   b) El grupo cíclico C_4 cuando $b^2 + 4b + 4 - 4a^2$ no es un cuadrado, pero sí lo es $(b^2 + 4b + 4 - 4a^2)(a^2 - 4b + 8)$.

   c) El grupo diédrico D_8 en cualquier otro caso.

6. Calcular el grupo de Galois de la cuártica bicuadrada genérica $x^4 + ax^2 + b$ sobre los números racionales.

7. Calcular el grupo de Galois de la cuártica recíproca genérica $x^4 + ax^3 + bx^2 + ax + 1$ sobre los números racionales.

8. Sea G el grupo de Galois de una cuártica separable $p_4(x)$ con coeficientes en un cuerpo k. Si $p_4(x)$ no es irreducible en $k[x]$, probar las siguientes afirmaciones:

   a) Si $p_4(x)$ tiene más de dos raíces en k, entonces $G = \{id\}$.

   b) Si $p_4(x)$ tiene dos raíces en k, entonces $G = S_2 = \{id, (12)\}$.

   c) $p_4(x)$ tiene una raíz en k, entonces $G = A_3$ ó $G = S_3$, según que el discriminante de $p_4(x)$ sea un cuadrado en k o no lo sea.

   d) Si $p_4(x)$ no tiene raíces en k, entonces $G = \{id, (12)(34)\}$ ó

   $$G = \{id, (12), (34), (12)(34)\}$$

9. Calcular el grupo de Galois sobre $\mathbb{Q}$ de las cuárticas: $x^4 - 4x^2 + 2$, $x^4 + 6x^2 + 1$, $x^4 - 3x + 1$, $2x^4 + x^3 - x^2 + 2x - 1$, $x^4 + 1$, $12x^4 + 8x^3 + 1$, $x^4 - 3x^3 + 4x^2 - 2x + 1$, $x^4 - 3x^3 - 3x^2 + 10x - 3$.

10. Hallar una cuártica con coeficientes racionales cuyo grupo de Galois sea $G = \{id, (12)(34)\}$ y otra cuyo grupo de Galois sea $G = \{id, (12), (34), (12)(34)\}$.

11. Determinar si las raíces de la unidad $e^{\frac{2\pi i}{7}}$, $e^{\frac{2\pi i}{8}}$, $e^{\frac{2\pi i}{9}}$, $e^{\frac{2\pi i}{10}}$, $e^{\frac{2\pi i}{11}}$, $e^{\frac{2\pi i}{12}}$, $e^{\frac{2\pi i}{13}}$, $e^{\frac{2\pi i}{14}}$, $e^{\frac{2\pi i}{15}}$ y $e^{\frac{2\pi i}{16}}$ son irracionales cuadráticos.

Solución de los problemas del curso

Solución de los problemas del capítulo primero

Problema 1. 1. $(x) \cap (y) = (x \cdot y) \subset \mathbb{Q}[x, y]$, no es ideal primo.

2. $I := (x) \cup (y) \subset \mathbb{Q}[x, y]$, no es ideal porque $x, y \in I$ y $x + y \notin I$.

3. Consideremos el morfismo de inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}[x]$, $n \mapsto n$. La imagen de $2\mathbb{Z}$ que es $2\mathbb{Z}$ no es un ideal de $\mathbb{Z}[x]$, porque $2 \in 2\mathbb{Z}$ y $2 \cdot x \notin 2\mathbb{Z}$.

Problema 2. Consideremos el morfismo de anillos $f\colon k[x_1, \ldots, x_n] \to k$, $f(p(x_1, \ldots, x_n)) = p(a_1, \ldots, a_n)$. El morfismo f es epiyectivo porque dado $a \in k$, $f(a) = a$. Los polinomios $x_i - a_i$ pertenecen a $\operatorname{Ker} f$, luego $(x_1 - a_1, \ldots, x_n - a_n) \subseteq \operatorname{Ker} f$. Por tanto, tenemos el epimorfismo

$$\bar{f}\colon k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n) \to k,\ \bar{f}(\overline{p(x_1, \ldots, x_n)}) = p(a_1, \ldots, a_n)$$

Si $\overline{p(x_1, \ldots, x_n)} \in \operatorname{Ker} \bar{f}$, entonces $p(a_1, \ldots, a_n) = 0$. Observemos que $\bar{x}_i = \bar{a}_i \in k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n)$, luego $\overline{p(x_1, \ldots, x_n)} = \overline{p(a_1, \ldots, a_n)} = 0$. En conclusión, $\operatorname{Ker} \bar{f} = 0$ y $\bar{f}$ es un isomorfismo. Además, $\operatorname{Ker} f = (x_1 - a_1, \ldots, x_n - a_n)$, luego $(x_1 - a_1, \ldots, x_n - a_n)$ coincide con el conjunto de todos los polinomios $p(x_1, \ldots, x_n)$ tales que $p(a_1, \ldots, a_n) = 0$. Por último, $(x_1 - a_1, \ldots, x_n - a_n)$ es un ideal maximal porque al hacer cociente por él se obtiene un cuerpo.

Problema 4. Si $I = A$, entonces existen $c_1(x_1, \ldots, x_n), \ldots, c_r(x_1, \ldots, x_n) \in A$ tales que $\sum_i c_i(x_1, \ldots, x_n) \cdot p_i(x_1, \ldots, x_n) = 1$. Por tanto, si el sistema de ecuaciones admite una solución $x_1 = \alpha_1, \ldots, x_n = \alpha_n$ en alguna extensión L de k, tendremos que $1 = \sum_i c_i(\alpha_1, \ldots, \alpha_n) \cdot p_i(\alpha_1, \ldots, \alpha_n) = 0$ y hemos llegado a contradicción.

Si $I \neq A$ sea $\mathfrak{m} \subset A$ un ideal maximal que contenga a I y $L = A/\mathfrak{m}$. Consideremos el morfismo de paso al cociente

$$\begin{array}{rcl} A & \to & A/\mathfrak{m} = L \\ x_i & \mapsto & \bar{x}_i \\ p(x_1, \ldots, x_n) & \mapsto & \overline{p(x_1, \ldots, x_n)} = p(\bar{x}_1, \ldots, \bar{x}_n) \end{array}$$

Entonces, $0 = \overline{p_i(x_1, \ldots, x_n)} = p_i(\bar{x}_1, \ldots, \bar{x}_n)$, luego $(\bar{x}_1, \ldots, \bar{x}_n) \in L^n$ es una solución del sistema de ecuaciones.

Problema 5. Si $(g)_0 \subseteq (f)_0$ todo ideal primo que contiene a g contiene a f. Por tanto, todos los ideales primos de $A/(g)$ contienen a $\bar{f}$. Luego, $\bar{f}$ es nilpotente en $A/(g)$, es decir, existe $n \in \mathbb{N}$ de modo que $\bar{0} = \bar{f}^n = \overline{f^n}$. Es decir, $f^n \in (g)$, o lo que es lo mismo g divide a f^n.

Si $f^n = g \cdot h$ entonces, $(f)_0 = (f^n)_0 = (g \cdot h)_0 = (g)_0 \cup (h)_0$ y $(g)_0 \subseteq (f)_0$.

Problema 6. $(\mathfrak{a})_0 = \operatorname{Spec} A$ si y sólo si a pertenece a todo ideal primo, es decir, $\mathfrak{a} \subseteq \prod_{x \in \operatorname{Spec} A} \mathfrak{p}_x = \operatorname{rad} A$.

Problema 7. $\frac{a}{1} = 0 = \frac{0}{1}$ en A_S si y sólo si existe $s \in S$ tal que $sa = 0$.

Problema 8. Sea $S = \{\bar{1}, \bar{2}, \bar{4}\} \subset \mathbb{Z}/6\mathbb{Z}$. El morfismo de localización $\mathbb{Z}/6\mathbb{Z} \to (\mathbb{Z}/6\mathbb{Z})_S$ no es inyectivo, por el ejercicio anterior.

Problema 9. Tenemos la inclusión $\mathbb{Z}[x] \hookrightarrow \mathbb{Q}(x)$. La imagen de todo elemento no nulo de $\mathbb{Z}[x]$ es invertible. Por la propiedad universal de la localización tenemos el morfismo de cuerpos $\mathbb{Z}[x]_{\mathbb{Z}[x]-\{0\}} \to \mathbb{Q}(x)$, $\frac{p(x)}{q(x)} \mapsto \frac{p(x)}{q(x)}$, que ha de ser inyectivo. Es epiyectivo: Dada una fracción $\frac{r(x)}{s(x)} \in \mathbb{Q}(x)$, existen $n, m \in \mathbb{Z}$ tales que $r'(x) = n \cdot r(x)$, $s'(x) = m \cdot s(x) \in \mathbb{Z}[x]$. Obviamente, $\frac{m \cdot r'(x)}{n \cdot s'(x)} \mapsto \frac{r(x)}{s(x)}$.

En conclusión, $\mathbb{Z}[x]_{\mathbb{Z}[x]-\{0\}} = \mathbb{Q}(x)$.

$\mathbb{Z}[\alpha] \subset \mathbb{C}$ es un anillo íntegro, incluido en $\mathbb{Q}(\alpha)$. De nuevo, el cuerpo de fracciones de $\mathbb{Z}[\alpha]$ está incluido en $\mathbb{Q}(\alpha)$ y argumentando igual antes se tiene la igualdad.

Problema 10. 1. Por la propiedad universal de la localización, el morfismo $A \to B_S$, $a \mapsto \frac{f(a)}{1}$, factoriza vía $A_S \to B_S$, $\frac{a}{s} \mapsto \frac{f(a)}{f(s)}$. Tenemos el morfismo $f\colon B \otimes_A A_S \to B_S$, $f(b \otimes \frac{a}{s}) = \frac{b}{1} \cdot \frac{f(a)}{f(s)}$.

Por la propiedad universal de la localización, el morfismo $B \to B \otimes_A A_S$, $b \mapsto b \otimes 1$, factoriza vía $g\colon B_S \to B \otimes_A A_S$, $g(\frac{b}{f(s)}) = b \otimes \frac{1}{s}$.

Los morfismos f y g son inversos entre sí.

2. $(A_S)_{S'} = A_S \otimes_A A_{S'}$. Tenemos morfismos naturales $A_S \to A_{S \cdot S'}$, $\frac{a}{s} \mapsto \frac{a}{s}$ y $A_{S'} \to A_{S \cdot S'}$, $\frac{a}{s'} \mapsto \frac{a}{s'}$. Sea $f\colon A_S \otimes_A A_{S'} \to A_{SS'}$, $f(\frac{a}{s} \otimes \frac{a'}{s'}) := \frac{a}{s} \cdot \frac{a'}{s'}$.

Por la propiedad universal de la localización, el morfismo $A \to A_S \otimes_A A_{S'}$, $a \mapsto a \otimes 1$, factoriza vía $g\colon A_{SS'} \to A_S \otimes_A A_{S'}$, $\frac{a}{ss'} \mapsto (a \otimes 1) \cdot (\frac{1}{s} \otimes \frac{1}{s'}) = \frac{a}{s} \otimes \frac{1}{s'}$.

Los morfismos f y g son inversos entre sí.

Problema 11. Consideremos el morfismo de localización $i\colon A \to A_S$ y sea $I := i^{-1}(J) = \{a \in A\colon \frac{a}{1} \in J\}$. Obviamente, $I \cdot A_S \subseteq J$. Dado $\frac{a}{s} \in J$, entonces $\frac{a}{1} = \frac{s}{1} \cdot \frac{a}{s} \in J$, luego $a \in I$. Por tanto, $a \cdot \frac{1}{s} = \frac{a}{s}$, $\frac{a}{s} \in I \cdot A_S$ y $I \cdot A_S = J$.

Observación: $I \cdot A_S = \{\frac{i}{s}\colon i \in I,\ s \in S\}$.

Problema 12. Observemos que $\mathfrak{p} \cdot A_S \neq A_S$: Si $\mathfrak{p} \cdot A_S = A_S$, entonces existen $p \in \mathfrak{p}$ y $s \in S$ tales que $\frac{p}{s} = \frac{1}{1}$. Entonces, existe $t \in S$ tal que $t \cdot p = 1$, luego $1 \in \mathfrak{p}$ y hemos llegado a contradicción. Si $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \in \mathfrak{p} \cdot A_S = \{\frac{p}{s'}\colon p \in \mathfrak{p},\ s' \in S\}$, entonces existe $t' \in S$, tal que $t'ab \in \mathfrak{p}$. Como $t' \notin \mathfrak{p}$ y $\mathfrak{p}$ es primo, $a \in \mathfrak{p}$ ó $b \in \mathfrak{p}$. Luego, $\frac{a}{s} \in \mathfrak{p} \cdot A_S$ ó $\frac{b}{t} \in \mathfrak{p} \cdot A_S$.

Problema 13. Si $\mathfrak{p} \subset A$ es un ideal primo, tal que $\mathfrak{p} \cap S = \emptyset$, entonces $\mathfrak{p} \cdot A_S$ es un ideal primo de A_S. Se cumple que $i^{-1}(\mathfrak{p} \cdot A_S) = \mathfrak{p}$: Obviamente, $\mathfrak{p} \subset i^{-1}(\mathfrak{p} \cdot A_S)$. Veamos la inclusión inversa. Si $a \in i^{-1}(\mathfrak{p} \cdot A_S)$, entonces $\frac{a}{1} \in \mathfrak{p} \cdot A_S$, luego existe $s \in S$ de modo que $s \cdot a \in \mathfrak{p}$, luego $a \in \mathfrak{p}$.

Si $\mathfrak{q} \subset A_S$ es un ideal primo, entonces $i^{-1}(\mathfrak{q})$ es un ideal primo de A, que no corta con S (porque si $s \in i^{\mathfrak{q}} \cap S$, entonces $\frac{s}{1} \in \mathfrak{q}$, que es invertible, luego $\mathfrak{q} = A_S$, lo cual es contradictorio). Veamos que $i^{-1}(\mathfrak{q}) \cdot A_S = \mathfrak{q}$. Obviamente, $i^{-1}(\mathfrak{q}) \cdot A_S \subseteq \mathfrak{q}$. Veamos la inclusión inversa. Dado $\frac{q}{s} \in \mathfrak{q}$, entonces $\frac{q}{1} \in \mathfrak{q}$, luego $q \in i^{-1}(\mathfrak{q})$ y $\frac{q}{s} = q \cdot \frac{1}{s} \in i^{-1}(\mathfrak{q}) \cdot A_S$.

En conclusión, $\operatorname{Spec} A_S \overset{i^*}{=} \{x \in \operatorname{Spec} A\colon \mathfrak{p}_x \cap S = \emptyset\}$, porque las asignaciones $\mathfrak{q} \mapsto i^{-1}(\mathfrak{q})$ y $\mathfrak{p} \mapsto \mathfrak{p} \cdot A_S$ son inversas entre sí.

Problema 14. Escribamos $M = \oplus^I A$ y $N = \oplus^J A$. Entonces,

$$M \otimes_A N = (\oplus^I A) \otimes_A N = \oplus^I (A \otimes_A N) = \oplus^I N = \oplus^I (\oplus^J A) = \oplus^{I\times J} A$$

Dado $i \in I$, si denotamos $e_i = (0, \overset{i}{\dots}, 1, 0, \cdots) \in \oplus^I A$. Vía estos isomorfismos se tiene que $e_i \otimes e_j \mapsto e_{(i,j)}$.

Problema 15. Dado $m \otimes b \in M \otimes_A B$, tendemos que $m = \sum_i a_i m_i$, luego $m \otimes b = \sum_i m_i \otimes a_i b = \sum_i a - ib \cdot (m \otimes 1) \in \langle m_i \otimes 1 \rangle_{i\in I}$. Luego, $\{m_i \otimes 1\}_{i\in I}$ es un sistema generador del B-módulo $M \otimes_A B$.

Si $L = \oplus^I A$, entonces $L \otimes_A B = (\oplus^I A) \otimes_A B = \oplus^I A \otimes_A B = \oplus^I B$, es un B-módulo libre. Dado $i \in I$, si denotamos $e_i = (0, \overset{i}{\dots}, 1, 0, \cdots) \in \oplus^I A$. Vía estos isomorfismos se tiene que $e_i \otimes 1 \mapsto e_i$.

Problema 16. Es consecuencia inmediata del problema 15.

Problema 17. Las coordenadas de $e \otimes 1$ en la base $\{e_i \otimes 1\}_{1\le i\le n}$ son $(x_1, \dots, x_n)$: $e \otimes 1 = (\sum_i x_i e_i) \otimes 1 = \sum_i x_i \cdot (e_i \otimes 1)$.

Problema 18. La matriz asociada a $f \otimes \mathrm{Id}$ es $A = (a_{ij})$: $(f \otimes \mathrm{Id})(e_i \otimes 1) = f(e_i) \otimes 1 = \sum_j a_{ji} e'_j \otimes 1 = \sum_j a_{ji}(e'_j \otimes 1)$.

Problema 19. Dado un conjunto de A-módulos $\{M_j\}_{j\in J}$ y de submódulos $\{N_j \subseteq M_j\}_{j\in J}$, tenemos el submódulo $\oplus_{j\in J} N_j \subseteq \oplus_{j\in J} M_j$, $(n_j)_{j\in J} \mapsto (n_j)_{j\in J}$. Además, $(\oplus_{j\in J} M_j)/\oplus_{j\in J} N_j = \oplus_{j\in J} M_j/N_j$, $\overline{(m_j)_{j\in J}} \mapsto (\bar{m}_j)_{j\in J}$.

Dado un conjunto I y un A-módulo M denotemos $M^{(I)} = \oplus_I M$. Dado un morfismo de módulos $f\colon M \to N$, sea $f^{(I)}\colon M^{(I)} \to M'^{(I)}$, $f^{(I)}((m_i)_{i\in I}) = (f(m_i))_{i\in I}$. Se cumple que $\operatorname{Ker} f^{(I)} = (\operatorname{Ker} f)^{(I)}$, $\operatorname{Im} f^{(I)} = (\operatorname{Im} f)^{(I)}$ y $\operatorname{Coker} f^{(I)} = (\operatorname{Coker} f)^{(I)}$.

El problema es consecuencia de que si $N = \oplus_I A$, entonces $M \otimes_A N = M^{(I)}$ y dado un morfismo $f\colon M \to M'$, entonces $f \otimes \mathrm{Id}\colon M \otimes N \to M' \otimes N$ se identifica con $f^{(I)}$.

Problema 20. El morfismo $g \otimes \mathrm{Id}$ es epiyectivo: Sea $m_3 \otimes n \in M_3 \otimes N$. Sea $m_2 \in M_2$ tal que $g(m_2) = m_3$. Entonces, $(g \otimes \mathrm{Id})(m_2 \otimes n) = m_3 \otimes n$.

$\operatorname{Im}(f \otimes \mathrm{Id}) \subseteq \operatorname{Ker}(g \otimes \mathrm{Id})$: $(g \otimes \mathrm{Id}) \circ (f \otimes \mathrm{Id}) = (g \circ f) \otimes \mathrm{Id} = 0 \otimes \mathrm{Id} = 0$.

Tenemos pues un epimorfismo $\overline{g \otimes \mathrm{Id}}\colon (M_2 \otimes N)/\operatorname{Im}(f \otimes \mathrm{Id}) \to M_3$, $\overline{g \otimes \mathrm{Id}}(\overline{m_2 \otimes n}) = (g \otimes \mathrm{Id})(m_2 \otimes n) = g(m_2) \otimes n$. Veamos que es un isomorfismo: Sea $s\colon M_3 \otimes N \to (M_2 \otimes N)/\operatorname{Im}(f \otimes \mathrm{Id}) \to M_3$, definido por $s(m_3 \otimes n) = \overline{m_2 \otimes n}$, donde m_2 es cualquier elemento de M_2 tal que $g(m_2) = m_3$ ($g(m'_2) = m_3$, entonces $m_2 = m'_2 + m'$, con $m' \in \operatorname{Ker} g = \operatorname{Im} f$, luego $\overline{m_2 \otimes n} = \overline{m'_2 \otimes n} + \overline{m' \otimes n} = \overline{m'_2 \otimes n}$). Es claro que $s \circ \overline{g \otimes \mathrm{Id}} = \mathrm{Id}$ y que $\overline{g \otimes \mathrm{Id}} \circ s = \mathrm{Id}$.

En conclusión, $(M_2 \otimes N)/\operatorname{Im}(f \otimes \mathrm{Id}) = M_3$ y $\operatorname{Im}(f \otimes \mathrm{Id}) = \operatorname{Ker}(g \otimes \mathrm{Id})$.

Problema 21. Si tensorializamos la sucesión exacta

$$0 \to E' \to E \to E/E' \to 0$$

por $\otimes_k V$, obtenemos la sucesión exacta

$$0 \to E' \otimes_k V \to E \otimes_k V \to (E/E') \otimes_k V \to 0$$

Luego, $(E/E') \otimes_k V = (E \otimes_k V)/(E' \otimes_k V)$.

Problema 22. Si tensorializamos las sucesiones exactas

$$0 \to \operatorname{Ker} f \to E' \to \operatorname{Im} f \to 0, \quad 0 \to Imaf \to E$$

por $\otimes_k V$, obtenemos las sucesiones exactas

$$0 \to (\operatorname{Ker} f) \otimes_k V \to E' \otimes_k V \to (\operatorname{Im} f) \otimes_k V \to 0, \quad 0 \to (Imaf) \otimes_k V \to E \otimes_k V$$

De las que se deduce que $(\operatorname{Im} f) \otimes_k V = \operatorname{Im}(f \otimes \operatorname{Id})$ y que $(\operatorname{Ker} f) \otimes_k V = \operatorname{Ker}(f \otimes \operatorname{Id})$.

Problema 24. Los morfismos $A[x_1, \ldots, x_n] \otimes_A B \to B[x_1, \ldots, x_n]$, $p(x) \otimes b \mapsto b \cdot p(x)$ y $B[x_1, \ldots, x_n] \to A[x_1, \ldots, x_n] \otimes_A B$, $\sum_\alpha b_\alpha \otimes x^\alpha \mapsto \sum_\alpha x^\alpha \otimes b_\alpha$ son inversos entre sí.

Problema 25.

$$\begin{aligned} A[x_1, \ldots, x_n]/(p_1, \ldots, p_r) \otimes_A B &= (A[x_1, \ldots, x_n]/(p_1, \ldots, p_r) \otimes_{A[x_1, \ldots, x_n]} A[x_1, \ldots, x_n]) \otimes_A B \\ &= A[x_1, \ldots, x_n]/(p_1, \ldots, p_r) \otimes_{A[x_1, \ldots, x_n]} B[x_1, \ldots, x_n] \\ &= B[x_1, \ldots, x_n]/(p_1, \ldots, p_r) \cdot B[x_1, \ldots, x_n] \\ &= B[x_1, \ldots, x_n]/(p_1, \ldots, p_r) \end{aligned}$$

Problema 26. Si $N, N' \subseteq M$ son dos A-submódulos y denotamos $\bar{N} = \{\bar{n} \in M/N',\ \forall n \in N\}$, se cumple que $(M/N')/\bar{N} = M/(N + N')$. En efecto, el núcleo del epimorfismo $M/N' \to M/(N + N')$, $\bar{m} \mapsto \bar{m}$, es $\bar{N}$, porque si $\bar{m} = 0$ en $M/(N+N')$, entonces $m \in N+N'$, luego existen $n \in N$ y $n' \in N'$ tales que $m = n+n'$ y $\bar{m} = \overline{n+n'} = \bar{n}$ en M/N'. Por tanto, $(M/N')/\bar{N} = M/(N + N')$.

Ahora ya,

$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = (\mathbb{Z}/n\mathbb{Z})/m \cdot (\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})/\overline{m\mathbb{Z}} = \mathbb{Z}/(n\mathbb{Z} + m\mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$$

Problema 27. Podemos proceder como en 26, pero vamos a dar otra demostración. Los morfismos $A/I \otimes_A A/J \to A/(I + J)$, $\bar{a} \otimes \bar{b} \mapsto \overline{ab}$ y $A/(I + J) \to A/I \otimes_A A/J$, $\bar{a} \mapsto \bar{a} \otimes 1$, están bien definidos y son inversos entre sí.

Problema 28. Por el teorema chino de los restos $A/(IJ) = A/I \times A/J$. Por tanto,

$$M/IJM = M \otimes_A (A/(IJ)) = M \otimes_A (A/I \times A/J) = (M \otimes_A A/I) \oplus (M \otimes_A A/J) = M/IM \oplus M/JM$$

Problema 29. Sea $I\colon E^* \otimes_k \overset{p}{\cdots} \otimes_k E^* \otimes_k E \otimes_k \overset{q}{\cdots} \otimes_k E \to T^p_q E$, el morfismo definido por

$$I(w_1 \otimes \cdots \otimes w_p \otimes e_1 \otimes \cdots \otimes e_q)(f_1, \ldots, f_p, v_1, \ldots, v_p) = w_1(f_1) \cdots w_p(f_p) \cdot v_1(e_1) \cdots v_q(e_q),$$

$\forall w_1, \ldots, w_p, v_1, \ldots, v_p \in E^*$, $\forall e_1, \ldots, e_q, f_1, \ldots, f_p \in E$. Sea $\{e_i\}_{i \in I}$ una base de E y $\{w_i\}_{i \in I}$ la base dual de E^*. Entonces,

$$I(w_{i_1} \otimes \cdots \otimes w_{i_p} \otimes e_{j_1} \otimes \cdots \otimes e_{j_q})(e_{r_1}, \ldots, e_{r_p}, w_{s_1}, \ldots, w_{s_q}) = \delta_{i_1 r_1} \cdots \delta_{i_p r_p} \cdot \delta_{j_1 s_1} \cdots \delta_{j_q s_q}$$

Luego, $\{I(w_{i_1} \otimes \cdots \otimes w_{i_p} \otimes e_{j_1} \otimes \cdots \otimes e_{j_q})\}$ es la base estándar de $T^p_q E$ (fijada la base de E). Por lo tanto, I es un isomorfismo.

Problema 30. Sea $I\colon E^* \otimes F \to \operatorname{Hom}_k(E, F)$, el morfismo definido por $I(w \otimes f)(e) := w(e) \cdot f$, para todo $e \in E$ (y todo $w \in E^*$ y $f \in F$). Sea $\{e_i\}_{i \in I}$ una base de E, $\{w_i\}_{i \in I}$ la base dual de E^* y sea $\{f_j\}$ una base de F. Entonces, $\{w_i \otimes f_j\}_{(i,j) \in I \times J}$ es una base de $E^* \otimes F$. Se tiene que $I(w_i \otimes f_j)(e_k) = 0$, para $k \neq i$ y $I(w_i \otimes f_j)(e_i) = f_j$, para $k = i$; es decir, $\{I(w_i \otimes f_j)\}_{(i,j) \in I \times J}$ es la base estándar de $\operatorname{Hom}_k(E, F)$ (fijadas las bases de E y F). Por tanto, I es un isomorfismo.

Solución de los problemas del capítulo segundo

Problema 1. $\alpha+2=\overline{x+2}\in\mathbb{Q}[x]/(2x^3+4x^2-x-2)=A$ es invertible, si y sólo si $(\overline{x+2})=A$, es decir, $(x+2,2x^3+4x^2-x-2)=\mathbb{Q}[x]$. Por tanto, $\alpha+2$ es invertible en A si y sólo si $x+2$ y $2x^3+4x^2-x-2$ son primos entre sí, es decir, -2 no es raíz de $2x^3+4x^2-x-2$. Pero, $2\cdot(-2)^3+4\cdot(-2)^2-(-2)-2=0$, luego $\alpha+2$ no es invertible. $\alpha-2$ es invertible, porque 2 no es raíz de $2x^3+4x^2-x-2$.

Problema 2. Los polinomios x^3-x-1 y $x+2$ son primos entre sí y tenemos que

$$\frac{-1}{7}\cdot(x^3-x-1)+\frac{x^2-2x^2+3}{7}\cdot(x+2)=1$$

Tomando clases en $K=\mathbb{Q}[x]/(x^3-x-1)$, tenemos que $\frac{\alpha^2-2\alpha^2+3}{7}\cdot(\alpha+2)=1$, luego $\frac{1}{\alpha+2}=\frac{\alpha^2-2\alpha^2+3}{7}$.

- $(2+\alpha)^3=(2+\bar{x})^3=\overline{x^3+6x^2+12x+8}=\overline{6x^2+13x+9}\neq\bar{1}$ (pues una base de $\mathbb{Q}[x]/(x^3-x-1)$, es $\bar{1},\bar{x},\bar{x}^2$).

- El polinomio x^2-2 tiene alguna raíz en K, si y sólo si $\sqrt{2}\in K$, es decir, $\mathbb{Q}[\sqrt{2}]\subseteq K$. Pero esta inclusión es imposible porque $\dim_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}]=2$ no divide a $\dim_{\mathbb{Q}}K=3$.

- Consideremos el endomorfismo $\mathbb{Q}$-lineal $K\overset{(\alpha^2+1)\cdot}{K}$, $\mu\mapsto(\alpha^2+1)\cdot\mu$. Resulta que el polinomio característico de este endomorfismo anula a α^2+1. La matriz de este endomorfismo es

$$\begin{pmatrix}1&1&0\\0&2&1\\1&0&2\end{pmatrix}$$

y su polinomio característico es x^3-5x^2+8x-5.

Problema 3. Supongamos que $\mathbb{Q}(\sqrt{a})=\mathbb{Q}(\sqrt{b})$. Si $\sqrt{a}\in\mathbb{Q}$, entonces $\sqrt{b}\in\mathbb{Q}(\sqrt{a})=\mathbb{Q}$, luego $\frac{\sqrt{a}}{\sqrt{b}}\in\mathbb{Q}$ y a/b es un cuadrado en $\mathbb{Q}$. Si $\sqrt{a}\notin\mathbb{Q}$, entonces $\sqrt{b}\notin\mathbb{Q}$. Por tanto, $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{a})=2$ y $\sqrt{b}=c_1+c_2\cdot\sqrt{a}$, con $c_1,c_2\in\mathbb{Q}$ y $c_2\neq0$. Si elevamos al cuadrado, tenemos $b=(c_1^2+c_2^2a)+2c_1c_2\cdot\sqrt{a}$, luego $c_1c_2=0$ y $c_1=0$. En conclusión, $\frac{\sqrt{a}}{\sqrt{b}}=1/c_2\in\mathbb{Q}$ y a/b es un cuadrado en $\mathbb{Q}$.

Si $a/b=c^2$, con $c\in\mathbb{Q}$, entonces $\sqrt{a}=c\cdot\sqrt{b}$ y $\mathbb{Q}(\sqrt{a})=\mathbb{Q}(\sqrt{b})$.

Problema 4. El polinomio x^3-2 anula a $\sqrt[3]{2}$ y es irreducible porque si lo fuese tendría raíces racionales. Por tanto, x^3-2 es el polinomio mínimo anulador de $\sqrt[3]{2}$ y $\mathbb{Q}[x]/(x^3-2)\simeq\mathbb{Q}(\sqrt[3]{2})$. Por tanto, $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})=3$. $\mathbb{Q}(\sqrt{2})\not\subset\mathbb{Q}(\sqrt[3]{2})$, porque $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{2})=2$ no divide a $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})=3$.

El polinomio x^4-2 es irreducible por el criterio de Eisenstein y anula a $\sqrt[4]{2}$, por tanto es su polinomio mínimo anulador. Luego, $\mathbb{Q}[x]/(x^4-2)\simeq\mathbb{Q}(\sqrt[4]{2})$ y $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[4]{2})=2$. $\mathbb{Q}(\sqrt[3]{2})\not\subset\mathbb{Q}(\sqrt[4]{2})$, porque $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})=3$ no divide a $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[4]{2})=4$.

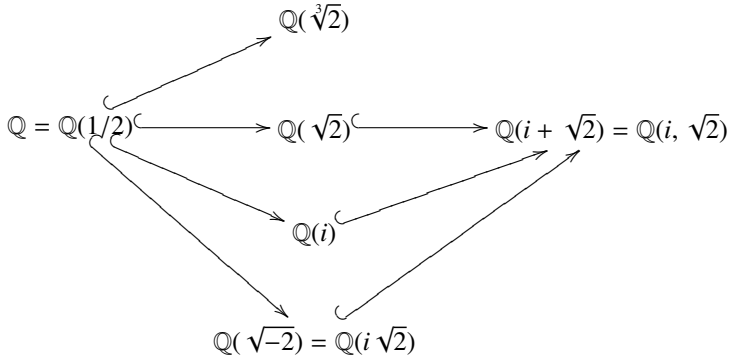
Problema 5. $\mathbb{Q}(\sqrt[4]{2},i\sqrt[4]{2})=\mathbb{Q}(\sqrt[4]{2},i)$, porque $\sqrt[4]{2},i\sqrt[4]{2}\in\mathbb{Q}(\sqrt[4]{2},i)$ y $\sqrt[4]{2},i\in\mathbb{Q}(\sqrt[4]{2},i\sqrt[4]{2})$.

$\mathbb{Q}(i\sqrt{2})=\mathbb{Q}[x]/(x^2+2)$, porque x^2+2 anula a $i\sqrt{2}$ y es irreducible. Por tanto, $\dim_{\mathbb{Q}}\mathbb{Q}(i\sqrt{2})=2$. $\mathbb{Q}(2^{-1/2},i)=\mathbb{Q}(\sqrt{2},i)$ es de grado 4 sobre $\mathbb{Q}$, porque $i\notin\mathbb{Q}(\sqrt{2})$ y tenemos la composición de extensiones $\mathbb{Q}\hookrightarrow\mathbb{Q}(\sqrt{2})\hookrightarrow\mathbb{Q}(\sqrt{2},i)$. Luego, $\mathbb{Q}(i\sqrt{2})\underset{\neq}{\mathbb{Q}}(\sqrt{2},i)$.

Una base del $\mathbb{Q}$-espacio vectorial $\mathbb{Q}(\sqrt{2},i)$, es $1,\sqrt{2},i,i\sqrt{2}$. Obviamente, $\mathbb{Q}(i+\sqrt{2})\subseteq\mathbb{Q}(\sqrt{2},i)$. Observemos que $(i+\sqrt{2})^2=1+2i\sqrt{2}$. Entonces, $1,i+\sqrt{2},1+2i\sqrt{2}\in\mathbb{Q}(i+\sqrt{2})$ y son linealmente

independientes. Luego, $\dim_{\mathbb{Q}} \mathbb{Q}(i+\sqrt{2}) = 4$ porque $\dim_{\mathbb{Q}} \mathbb{Q}(i+\sqrt{2}) \geq 3$ y divide a $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, i) = 4$. En conclusión, $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(i+\sqrt{2})$.

Problema 6.



Problema 7. Si $\alpha \in L$ es una raíz de $p(x)$, entonces $k[x]/(p(x)) \simeq k(\alpha) \hookrightarrow L$ y el grado de L sería divisible por el grado de $p(x)$.

Problema 8. Por el problema 7 $x^3 - 3$ no tiene raíces en $\mathbb{Q}(\sqrt{2})$. Por tanto, $x^3 - 3$ es el polinomio mínimo anulador de $\sqrt[3]{3}$ con coeficientes en $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ es una extensión de cuerpos de grado 3.

$$\begin{aligned}\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) &= \mathbb{Q}(\sqrt{2}) \cdot 1 \oplus \mathbb{Q}(\sqrt{2}) \cdot \sqrt[3]{3} \oplus \mathbb{Q}(\sqrt{2}) \cdot (\sqrt[3]{3})^2 \\ &= \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \sqrt{2} \oplus \mathbb{Q} \cdot \sqrt[3]{3} \oplus \mathbb{Q} \cdot \sqrt{2} \cdot \sqrt[3]{3} \oplus \mathbb{Q} \cdot \sqrt[3]{3}^2 \oplus \mathbb{Q} \cdot \sqrt{2} \cdot \sqrt[3]{3}^2\end{aligned}$$

Tenemos que

$$\begin{aligned}1 &= 1 \cdot 1 + 0 \cdot \sqrt{2} + 0 \cdot \sqrt[3]{3} + 0 \cdot \sqrt{2}\sqrt[3]{3} + 0 \cdot \sqrt[3]{3}^2 + 0 \cdot \sqrt{2}\sqrt[3]{3}^2 \\ \sqrt{2} + \sqrt[3]{3} &= 0 \cdot 1 + 1 \cdot \sqrt{2} + 1 \cdot \sqrt[3]{3} + 0 \cdot \sqrt{2}\sqrt[3]{3} + 0 \cdot \sqrt[3]{3}^2 + 0 \cdot \sqrt{2}\sqrt[3]{3}^2 \\ (\sqrt{2} + \sqrt[3]{3})^2 &= 2 \cdot 1 + 0 \cdot \sqrt{2} + 0 \cdot \sqrt[3]{3} + \cdot 2\sqrt{2}\sqrt[3]{3} + 1 \cdot \sqrt[3]{3}^2 + 0 \cdot \sqrt{2}\sqrt[3]{3}^2 \\ (\sqrt{2} + \sqrt[3]{3})^3 &= 3 \cdot 1 + 2 \cdot \sqrt{2} + 6 \cdot \sqrt[3]{3} + 0 \cdot \sqrt{2}\sqrt[3]{3} + 0 \cdot \sqrt[3]{3}^2 + 3 \cdot \sqrt{2}\sqrt[3]{3}^2 \\ (\sqrt{2} + \sqrt[3]{3})^4 &= 4 \cdot 1 + 12 \cdot \sqrt{2} + 3 \cdot \sqrt[3]{3} + 8 \cdot \sqrt{2}\sqrt[3]{3} + 12 \cdot \sqrt[3]{3}^2 + 0 \cdot \sqrt{2}\sqrt[3]{3}^2 \\ (\sqrt{2} + \sqrt[3]{3})^5 &= 60 \cdot 1 + 4 \cdot \sqrt{2} + 20 \cdot \sqrt[3]{3} + 15 \cdot \sqrt{2}\sqrt[3]{3} + 3 \cdot \sqrt[3]{3}^2 + 20 \cdot \sqrt{2}\sqrt[3]{3}^2 \\ (\sqrt{2} + \sqrt[3]{3})^6 &= 17 \cdot 1 + 120 \cdot \sqrt{2} + 90 \cdot \sqrt[3]{3} + 24 \cdot \sqrt{2}\sqrt[3]{3} + 60 \cdot \sqrt[3]{3}^2 + 18 \cdot \sqrt{2}\sqrt[3]{3}^2\end{aligned}$$

Los cuatro primeros son linealmente independientes, luego $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}+\sqrt[3]{3}) \geq 4$ y divide a 6. Por tanto, $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2} + \sqrt[3]{3}) = 6$ y $\mathbb{Q}(\sqrt{2} + \sqrt[3]{3}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. Tenemos que

$$\begin{pmatrix} 1 & 0 & 2 & 3 & 4 & 60 \\ 0 & 1 & 0 & 2 & 12 & 4 \\ 0 & 1 & 0 & 6 & 3 & 20 \\ 0 & 0 & 2 & 0 & 8 & 15 \\ 0 & 0 & 1 & 0 & 12 & 3 \\ 0 & 0 & 0 & 3 & 0 & 20 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 17 \\ 120 \\ 90 \\ 24 \\ 60 \\ 18 \end{pmatrix} = \begin{pmatrix} -1 \\ 36 \\ -12 \\ 6 \\ 6 \\ 0 \end{pmatrix}$$

Luego, el polinomio anulador de $\sqrt{2} + \sqrt[3]{3}$ resulta ser $x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1$.

Problema 9. K es un $\mathbb{F}_2$-espacio vectorial de dimensión 3, es isomorfo como $\mathbb{F}_2$-espacio vectorial a $\mathbb{F}_2^3$, que tiene $2^3 = 8$ elementos. $K^* = K - \{0\}$ es un grupo con la multiplicación de orden 7, luego es cíclico y está generado por cualquier elemento, distinto de 1. Luego, $K^* = \{\alpha, \alpha^2, \ldots, \alpha^7 = 1\}$.

Problema 10. $\mathbb{F}_2[x]/(x^2 + x + 1)$ y $\mathbb{F}_3[x]/(x^2 + 1)$.

Problema 11. Las raíces de $x^3 - 1$ son $\{e^{2\pi i/3}, e^{4\pi i/3}, e^{6\pi i/3} = 1\}$ y $\mathbb{Q}(e^{2\pi i/3}, e^{4\pi i/3}, e^{6\pi i/3}) = \mathbb{Q}(e^{2\pi i/3})$. Tenemos que $x^3 - 1 = (x - 1)(x^2 + x + 1)$. El polinomio $x^2 + x + 1$ es irreducible de raíces $e^{2\pi i/3}, e^{4\pi i/3}$. Luego el polinomio mínimo anulador de $e^{2\pi i/3}$ es $x^2 + x + 1$ y $\dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/3}) = 2$.

Observemos que α es una raíz de $x^3 - 1$ si y sólo si $-\alpha$ es una raíz de $x^3 + 1$. Luego, la $\mathbb{Q}$-subextensión de $\mathbb{C}$ generada por las raíces de $x^3 + 1$ coincide con $\mathbb{Q}(e^{2\pi i/3})$.

$\mathbb{Q}(e^{2\pi i/6})$ es la $\mathbb{Q}$-subextensión de $\mathbb{C}$ generada por las raíces de $x^6 - 1$. Como hemos dicho $\dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/6}) = 3$.

La $\mathbb{Q}$-subextensión de $\mathbb{C}$ generada por las raíces de $x^4 - 1$, es $\mathbb{Q}(e^{2\pi i/4})$. Además, $x^4 - 1 = (x^2 - 1)(x^2 + 1)$, $x^2 + 1$ es irreducible y $e^{2\pi i/4}$ es raíz de $x^2 + 1$. Luego, $\dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/4}) = 2$.

Observemos que $x^8 - 1 = (x^4 - 1) \cdot (x^4 + 1)$. Las raíces de $x^8 - 1$ son las potencias de $e^{2\pi i/8}$ y $e^{2\pi i/8}$ es raíz de $x^4 + 1$ (y no de $x^4 - 1$). Observemos que $\mathbb{Q}(e^{2\pi i/4} = i) \underset{\neq}{\subset} \mathbb{Q}(e^{2\pi i/8})$. Luego, $\dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/8}) = 2 \cdot m$, con $m > 1$. El polinomio anulador de $e^{2\pi i/8}$ divide a $x^4 + 1$ y es de grado $2 \cdot m$, luego es $x^4 + 1$. Por tanto, $\dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/8}) = 4$.

Observemos que $x^5 - 1 = (x - 1) \cdot (x^4 + x^3 + x^2 + x + 1)$. Además, si hacemos el cambio de variable $x = y + 1$, obtenemos

$$(x^4 + x^3 + x^2 + x + 1) = \frac{x^5 - 1}{x - 1} = \frac{(y + 1)^5 - 1}{y + 1 - 1} = y^4 + 5y^3 + 10y^2 + 10y + 5,$$

que es irreducible por el criterio de Eisenstein. Por tanto, $x^4 + x^3 + x^2 + x + 1$ es irreducible y la subextensión de $\mathbb{C}$ generada por sus raíces, $\mathbb{Q}(e^{2\pi i/5})$, es de grado 4.

Observemos que α es una raíz de $x^5 + 11$ si y sólo si $-\alpha$ es raíz de $x^5 - 1$, luego la subextensión de $\mathbb{C}$ generada por sus raíces es $\mathbb{Q}(e^{2\pi i/5})$

Problema 12. Por el criterio de Eisenstein, $x^n - 2$ es irreducible. Luego, $\mathbb{Q}(\sqrt[n]{2}) = \mathbb{Q}[x]/(x^n - 2)$ y su grado es n.

Problema 13. Las raíces de $x^3 - 2$ son $\sqrt[3]{2}, e^{2\pi i/3} \cdot \sqrt[3]{2}$ y $e^{4\pi i/3} \cdot \sqrt[3]{2}$. Luego,

$$\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3} \cdot \sqrt[3]{2}, e^{4\pi i/3} \cdot \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$$

y $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) = 3 \cdot 2 = 6$.

La $\mathbb{Q}$-subextensión generada por las raíces de $x^4 - 2$, es $\mathbb{Q}(\sqrt[4]{2}, i)$. Como $i \notin \mathbb{Q}(\sqrt[4]{2})$, entonces $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{2}, i) = 4 \cdot 2 = 8$.

La $\mathbb{Q}$-subextensión generada por las raíces de $x^4 + 2$, es

$$\mathbb{Q}(\sqrt[4]{2}, e^{2\pi i/8} \cdot \sqrt[4]{2}, e^{5\pi i/8} \cdot \sqrt[4]{2}, e^{7\pi i/8} \cdot \sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, e^{2\pi i/8}) = \mathbb{Q}(\sqrt[4]{2}, \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \cdot i) = \mathbb{Q}(\sqrt[4]{2}, i)$$

que es una extensión de grado 8.

Consideremos el polinomio $x^4 - x^2 + 1$. Sea $y = x^2$, las raíces de $y^2 - y + 1$, son $\frac{1 \pm \sqrt{3}i}{2}$. Luego las raíces de $x^4 - x^2 + 1$ son $\pm \sqrt{\frac{1 \pm \sqrt{3}i}{2}}$. La $\mathbb{Q}$-subextensión generada por las raíces de $x^4 - x^2 + 1$ es $\mathbb{Q}(\frac{\sqrt{3} \pm i}{2}) = \mathbb{Q}(\sqrt{3}, i)$ que es una extensión de grado 4.

Tenemos que $x^4 + x^2 - 2 = (x - 1)(x + 1)(x^2 + 2)$. Luego, La $\mathbb{Q}$-subextensión generada por las raíces de $x^4 + x^2 - 2$ es $\mathbb{Q}(\sqrt{-2})$, que es de grado 2.

Tenemos que $x^3 - 4x^2 + 5 = (x + 1)(x^2 - 5x + 5)$. Luego, La $\mathbb{Q}$-subextensión generada por las raíces de $x^3 - 4x^2 + 5$ es $\mathbb{Q}(\sqrt{5})$, que es de grado 2.

Problema 14. Como $i \notin \mathbb{Q}(\sqrt[4]{2})$, entonces $\mathbb{Q}(i, \sqrt[4]{2})$ es una $\mathbb{Q}$-extensión de grado 8, luego es una $\mathbb{Q}(i)$-extensión de grado 4. Por tanto, el polinomio mínimo anulador de $\sqrt[4]{2}$ con coeficientes en $\mathbb{Q}(i)$ es $x^4 - 2$.

$\mathbb{Q}(\sqrt[4]{2})$ es una $\mathbb{Q}(\sqrt{2})$-extensión de grado 2, luego el polinomio mínimo anulador de $\sqrt[4]{2}$ con coeficientes en $\mathbb{Q}(\sqrt{2})$ es $x^2 - \sqrt{2}$.

$\mathbb{Q}(\sqrt[4]{2}, \sqrt[3]{2})$ es una $\mathbb{Q}$-extensión de grado 12, luego es una $\mathbb{Q}(\sqrt[3]{2})$-extensión de grado 4. El polinomio mínimo anulador de $\sqrt[4]{2}$ con coeficientes en $\mathbb{Q}(\sqrt[3]{2})$ es $x^4 - 2$.

Problema 15. $\mathbb{Q}(\sqrt{2} + \sqrt[3]{3})$ es una $\mathbb{Q}$-extensión de grado 6, que no es una potencia de 2, luego $\sqrt{2} + \sqrt[3]{3}$ no es un irracional cuadrático. $\mathbb{Q}(\sqrt[5]{2})$ es una $\mathbb{Q}$-extensión de grado 5, que no es una potencia de 2, luego $\sqrt[5]{2}$ no es un irracional cuadrático. $\sqrt[4]{2} = \sqrt{\sqrt{2}}$, luego es un irracional cuadrático.

Problema 16. Sea $\alpha \in K - k$. Obviamente, $\{1, \alpha\}$ es una base del k-espacio vectorial K. Luego, existen $b, c \in k$ tales que $\alpha^2 = c \cdot 1 + b \cdot \alpha$ y $\alpha = \frac{b \pm \sqrt{b^2 - 4c}}{2}$ y $K = k(\alpha) = k(\sqrt{b^2 - 4c})$.

La $\mathbb{Z}/2\mathbb{Z}$-extensión $K = \mathbb{Z}/2\mathbb{Z}[x]/(x^2 + x + 1)$, no es extender por un radical cuadrático de 0 ó $1 \in \mathbb{Z}/2\mathbb{Z}$.

Problema 17. $x^2 + 1$ y $x^3 - 2$ son polinomios primos entre sí, luego

$$\mathbb{Q}[x]/((x^2 + 1) \cdot (x^3 - 2)) = \mathbb{Q}[x]/(x^2 + 1) \times \mathbb{Q}[x]/(x^3 - 2) = \mathbb{Q}(i) \times \mathbb{Q}(\sqrt[3]{2})$$

Problema 18. $x^2 + 1$ y $(x + 1)^2 + 1 = x^2 + 2x + 2$ son polinomios primos entre sí, luego

$$\mathbb{Q}[x]/((x^2 + 1)(x^2 + 2x + 2)) = \mathbb{Q}[x]/(x^2 + 1) \times \mathbb{Q}[x]/(x^2 + 2x + 2) = \mathbb{Q}(i) \times \mathbb{Q}(i)$$

Problema 19. Resulta del epimorfismo obvio $\mathbb{Q}(\alpha_1) \otimes_{\mathbb{Q}} \cdots \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha_n) \to \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ y de los epimorfismos $\mathbb{Q}[x]/(p_i(x)) \to \mathbb{Q}(\alpha_i)$, $\overline{q(x)} \mapsto q(\alpha_i)$.

Problema 20. Consideremos el epimorfismo $L \otimes_k L \to L$, $l \otimes l' \mapsto l \cdot l'$. Todo morfismo entre cuerpos es inyectivo (o nulo). Por tanto, si $L \otimes_k L$ es un cuerpo entonces $L \otimes_k L = L$. Entonces, el morfismo $L \to L \otimes_k L$, $l \mapsto l \otimes 1$ es un isomorfismo, porque es el morfismo inverso. Ahora bien, si $\{e_1 = 1, \ldots, e_n\}$ es una base del k-espacio vectorial L, entonces $\{e_i \otimes e_j\}$ es una base de L. Tenemos que $\{e_i \otimes 1\}$ es una base de $L \otimes_k L$. En conclusión, L es un k-espacio vectorial de dimensión 1, luego $L = k$.

Si $L = k$, entonces $L \otimes_k L = k \otimes_k k = k$, que es cuerpo.

Problema 21. $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$ no es cuerpo y $\mathbb{Q}(\sqrt{2}) \otimes \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ es cuerpo.

Problema 22. $\mathbb{C}$ es un cuerpo algebraicamente cerrado, por tanto si $\mathbb{C} \hookrightarrow K$ es una extensión finita de cuerpos, toda $\alpha \in K$ es algebraico sobre $\mathbb{C}$, luego $\alpha \in \mathbb{C}$ y $K = \mathbb{C}$. Toda k-álgebra finita reducida es producto directo de extensiones finitas de cuerpos de k. Por tanto, toda $\mathbb{C}$-álgebra finita reducida es trivial. $\mathbb{C}[x]/(x^2)$ es una $\mathbb{C}$-álgebra finita con nilpotentes, luego no trivial.

Problema 23. Sea $\mathbb{R} \hookrightarrow K$ una extensión finita de $\mathbb{R}$. Entonces, $K \otimes_{\mathbb{R}} \mathbb{C}$ es una $\mathbb{C}$-álgebra finita racional (es más trivial). Luego, $\mathrm{Hom}_{\mathbb{R}}(K, \mathbb{C}) = \mathrm{Hom}_{\mathbb{C}}(K \otimes_{\mathbb{R}} \mathbb{C}, \mathbb{C}) \neq \emptyset$ y tenemos un morfismo de $\mathbb{R}$-algebras $K \hookrightarrow \mathbb{C}$. Por dimensiones, $K = \mathbb{R}$ ó $K = \mathbb{C}$. Toda k-álgebra finita reducida es producto directo de extensiones finitas de cuerpos de k. Por tanto, toda $\mathbb{R}$-álgebra finita reducida es isomorfa a $\mathbb{R} \oplus \overset{n}{\ldots} \oplus \mathbb{R} \oplus \mathbb{C} \oplus \overset{m}{\ldots} \oplus \mathbb{C}$ para ciertos $n, m \in \mathbb{N}$.

Problema 24. Sea $L \cdot L'$ un compuesto de L y L'. Tenemos que $L \hookrightarrow L \cdot L'$, luego el grado de $L \cdot L'$ es múltiplo de L. Igualmente, el grado de $L \cdot L'$ es múltiplo de L'. Por tanto, el grado de $L \cdot L'$ es múltiplo de el grado de L por el de L'. Tenemos un epimorfismo $L \otimes_k L' \to L \cdot L'$. $L \otimes_k L'$ es un k-espacio vectorial de dimensión el grado de L por el de L'. Por tanto, $L \otimes_k L' = L \cdot L'$.

Problema 25. Dado un polinomio irreducible $p(x)$ de raíces $\alpha_1, \ldots, \alpha_n$, entonces $\mathrm{Aut}_{k-alg}\, k(\alpha_1) = \{\alpha_i \colon \alpha_i \in k(\alpha_1)\}$, $\tau \mapsto \tau(\alpha_1)$.

$\mathrm{Aut}_{\mathbb{Q}-alg}\, \mathbb{Q}(\sqrt{2}) = \{\sqrt{2}, -\sqrt{2}\}$.

$\mathrm{Aut}_{\mathbb{Q}-alg}\, \mathbb{Q}(\sqrt[3]{2}) = \{\mathrm{Id}\}$, porque $e^{2\pi i/3} \cdot \sqrt[3]{2}, e^{4\pi i/3} \cdot \sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$.

$\mathrm{Aut}_{\mathbb{Q}-alg}\, \mathbb{Q}(\sqrt[4]{2}) = \{\sqrt[4]{2}, -\sqrt[4]{2}\}$, porque $\pm\sqrt[4]{2} \cdot i \notin \mathbb{Q}(\sqrt[4]{2})$.

$\mathrm{Aut}_{\mathbb{Q}-alg}\, \mathbb{Q}(\sqrt[5]{2}) = \{\mathrm{Id}\}$, porque $e^{n\cdot 2\pi i/5} \cdot \sqrt[5]{2} \notin \mathbb{Q}(\sqrt[5]{2})$, para $n = 1, 2, 3, 4$.

$\mathrm{Aut}_{\mathbb{Q}-alg}\, \mathbb{Q}(\sqrt[6]{2}) = \{\pm\sqrt[6]{2}\}$, porque $e^{n\cdot 2\pi i/6} \cdot \sqrt[5]{2} \notin \mathbb{Q}(\sqrt[6]{2})$, para $n = 1, 2, 4, 5$.

Problema 26. El cuerpo de descomposición de $x^3 - 2$ es $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) = \mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/3})$. Sea $\tau \in \mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ determinado por $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, $\tau(e^{2\pi i/3}) = e^{4\pi i/3}$. Entonces,

$$\mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) = \mathrm{Aut}_{\mathbb{Q}(e^{2\pi i/3})}\, \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) \coprod \mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) \circ \tau$$

Por último, $\mathrm{Aut}_{\mathbb{Q}(e^{2\pi i/3})}\, \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) = \{\sigma_0, \sigma_1, \sigma_2\}$, con $\sigma_j(\sqrt[3]{2}) := e^{j\cdot 2\pi i/3} \cdot \sqrt[3]{2}$.

El cuerpo de descomposición de $x^4 - 2$ es $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(i)$. Entonces, $\mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt[4]{2}, i)) = \{\tau_{rs}\}_{1\leq r,s\leq 2}$, con $\tau_{rs}(i) = (-1)^r \cdot i$ y $\tau_{rs}(\sqrt[4]{2}) = (-1)^s \cdot i \cdot \sqrt[4]{2}$.

Problema 27. $\mathbb{Q}(\sqrt[5]{5}, e^{2\pi i/5})$ es una extensión de grado 20 sobre $\mathbb{Q}$, luego es una $\mathbb{Q}(\sqrt[5]{5})$-extensión de grado 4 y el polinomio mínimo anulador de $e^{2\pi i/5}$) con coeficientes en $\mathbb{Q}(\sqrt[5]{5})$ es $x^4 + x^3 + x^2 + x + 1$.

$$\mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt[5]{5}, e^{2\pi i/5})) = \{\tau_{rs}\}_{1\leq r\leq 4; 1\leq s\leq 5},$$

con $\tau_{rs}(e^{2\pi i/5}) = e^{r\cdot 2\pi i/5}$ y $\tau_{rs}(\sqrt[5]{5}) = e^{s\cdot 2\pi i/5} \cdot \sqrt[5]{5}$.

Problema 28. Escribamos $p(x) = (x-alpha)^m \cdot q(x)$, con $q(\alpha) \neq 0$. Entonces, $p'(x) = m\cdot(x-\alpha)^{m-1} q(x) + (x-\alpha)^m \cdot q'(x) = (x-alpha)^{m-1} \cdot (mq(x) + (x-\alpha)q'(x))$, que es de multiplicidad $m-1$ en característica cero y de multiplicidad mayor o igual que $m-1$ en característica prima (observemos que $m = 0 \in k$, si $m \in \mathbb{N}$ es múltiplo de la característica). Si $m = 1$, entonces α no es raíz de $p'(x)$.

Problema 29. Es inmediato por el problema 28.

Problema 30. Las raíces múltiples de $p(x)$ son las raíces de $m.c.d.(p(x), p'(x))$. Si hay raíces múltiples, entonces $m.c.d(p(x), p'(x))$ es un polinomio de grado mayor que cero. Si $p'(x) \neq 0$, entonces $m.c.d(p(x), p'(x))$ es un polinomio de grado menor que el de $p(x)$, que lo divide. En este caso, $p(x)$ no sería irreducible y llegamos a contradicción.

Si $p'(x) = 0$, entonces $m.c.d.(p(x), p'(x)) = p(x)$ y todas las raíces son de $p(x)$ son múltiples. Si $p'(x) \neq 0$, entonces $m.c.d.(p(x), p'(x)) = (1)$ y $p(x)$ no tiene raíces múltiples.

Problema 31. Sea $p(x) = x^4 + 4x^2 + 1 \in k[x]$, entonces $p'(x) = 4x^3 + 8x = 4x(x^2 + 2)$ que es primo con $p(x)$ si $k = \mathbb{Q}, \mathbb{F}_2$, luego $p(x)$ no tiene raíces múltiples sobre estos cuerpos. Sobre $\mathbb{F}_3$, $x^2 + 2 = x^2 - 1 = (x + 1)(x - 1)$. Las raíces comunes son el ± 1. Luego, ± 1 son raíces de $p(x)$ de multiplicidad 2. Sobre $\mathbb{F}_5$, $p(x)$ y $x^2 + 2$ son primos entre sí, luego $p(x)$ no tiene raíces múltiples.

Sea $p(x) = 4x^4 - 4x^3 - 3x^2 + 2x + 1$, entonces $p'(x) = 16x^3 - 12x^2 - 6x + 2$. Sobre $\mathbb{Q}$ y $\mathbb{F}_5$ se tiene que $m.c.d(p(x), p'(x)) = 2x^2 - x - 1 = 2(x-1)(x+1/2)$, luego $1, 1/2$ son las raíces múltiples, de multiplicidad 2. Sobre $\mathbb{F}_2$, $p(x) = x^2 - x + 1 = (x + 1)^2$, que tiene -1 como raíz múltiple de multiplicidad 2. Sobre $\mathbb{F}_3$, $m.c.d(p(x), p'(x)) = p'(x) = x^3 - 1 = (x - 1)^3$ y $p(x) = (x - 1)^4$, luego 1 es de multiplicidad 4.

Solución de los problemas del capítulo tercero

Problema 1. Sea una extensión de cuerpos $k \hookrightarrow k(\alpha)$ separable y $p(x)$ el polinomio mínimo anulador de α, con coeficientes en k. Entonces, $k(\alpha) = k[x]/(p(x))$. Si $\alpha_1, \ldots, \alpha_n$ son las raíces de $p(x)$, entonces una extensión Σ trivializa a $k(x)/(p(x)$ si y sólo si $\alpha_1, \ldots, \alpha_n \in \Sigma$.

El polinomio mínimo anulador de $\sqrt[3]{2}$ es $x^3 - 2$, cuyas raíces son $\sqrt[3]{2}$, $\sqrt[3]{2} \cdot e^{2\pi i/3}$, $\sqrt[3]{2} \cdot e^{4\pi i/3}$. La mínima extensión trivializante de $\mathbb{Q}(\sqrt[3]{2})$, es

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2} \cdot e^{2\pi i/3}, \sqrt[3]{2} \cdot e^{4\pi i/3}) = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$$

El polinomio mínimo anulador de $\sqrt[4]{2}$ es $x^4 - 2$, cuyas raíces son $\sqrt[4]{2}$, $\sqrt[4]{2} \cdot e^{2\pi i/4}$, $\sqrt[4]{2} \cdot e^{4\pi i/4}$, $\sqrt[4]{2} \cdot e^{6\pi i/4}$. La mínima extensión trivializante de $\mathbb{Q}(\sqrt[4]{2})$, es

$$\mathbb{Q}(\sqrt[4]{2}, i)$$

Si $A = A_1 \times A_2$ y K_1 trivializa a A_1 y K_2 trivializa a A_2, entonces cualquier compuesto de K_1 y K_2 trivializa a A. Entonces,

$$\mathbb{Q}(i) \cdot \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) = \mathbb{Q}(i, e^{2\pi i/3}, \sqrt[3]{2})$$

Problema 2. $k(\alpha^p) \hookrightarrow k(\alpha)$ es separable, porque α es separable sobre k. El polinomio $x^p - \alpha^p \in k(\alpha^p)[x]$ anula a α, y tiene a α como única raíz (múltiple), pues $x^p - \alpha^p = (x - \alpha)^p$. En conclusión, el polinomio mínimo anulador de α con coeficientes en $k(\alpha^p)$, que es separable y divide a $x^p - \alpha^p$, ha de ser $x - \alpha$, es decir, $\alpha \in k(\alpha^p)$ y $k(\alpha^p) = k(\alpha)$.

Problema 3. En característica cero, las k-álgebras finitas reducidas coinciden con las separables. Además, el producto tensorial de k-álgebras finitas separables es separable.

Problema 4. El anillo $A = \mathbb{F}_2[t]$ es un dominio de factorización única. Por el criterio de Eisenstein $x^2 - t \in A[x]$ es irreducible. Por el lema de Gauss, $x^2 - t \in \mathbb{F}_2(t)[x] = k[x]$ es irreducible.

Tenemos que $(x - \alpha)^2 = x^2 - \alpha^2 = x^2 - t$. Por tanto, α es una raíz doble del polinomio irreducible $x^2 - t \in k[x]$, luego $k \hookrightarrow k(\alpha) = k[\sqrt{t}]$ no es separable.

Problema 5. Dado $p(x) \in \mathbb{C}$, todas sus raíces $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, luego $\mathbb{C}(\alpha_1, \ldots, \alpha_n) = \mathbb{C}$, cuyo grupo de Galois sobre $\mathbb{C}$ es $G = \{1\}$.

Problema 6. Efectivamente.

Problema 7. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es el cuerpo de descomposición de $(x^2-2)\cdot(x^2-3) \in \mathbb{Q}[x]$, luego es de Galois. Además, $\sqrt{3} \not\in \mathbb{Q}(\sqrt{2})$, por tanto, $\mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$ es de grado 2, luego $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es una $\mathbb{Q}$-extensión de grado 4. Luego el grupo G de Galois de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es de orden 4. Todo $\tau \in G$ está determinado por valor en $\sqrt{2}$ y en $\sqrt{3}$. Además, se cumple que $\tau(\sqrt{2}) = \pm\sqrt{2}$ y $\tau(\sqrt{3}) = \pm\sqrt{3}$. En conclusión,

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq G,\ (\bar{i}, \bar{j}) \mapsto \tau_{\bar{i}\bar{j}},\ \text{donde } \tau_{\bar{i}\bar{j}}(\sqrt{2}) := (-1)^i\sqrt{2},\ \text{y } \tau_{\bar{i}\bar{j}}(\sqrt{3}) := (-1)^j\sqrt{3}$$

Si $k \hookrightarrow K$ es una extensión de Galois, $\alpha \in K$ y el polinomio mínimo anulador de α es $p(x)$ de raíces $\alpha_1, \ldots, \alpha_n$, entonces $\alpha_1, \ldots, \alpha_n \in K$. El polinomio anulador con coeficientes en $\mathbb{Q}$ de $\sqrt[3]{3}$ es $x^3 - 3$ y $e^{2\pi i/3}\cdot\sqrt[3]{3}$. Se cumple que $e^{2\pi i/3}\cdot\sqrt[3]{3} \not\in \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$, luego $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ no es Galois.

$\mathbb{Q}(i\cdot\sqrt{2}, \sqrt[3]{3})$ es una $\mathbb{Q}$-extensión de grado 6, porque un compuesto de las extensiones $\mathbb{Q}(i\cdot\sqrt{2}$ y $\mathbb{Q}(\sqrt[3]{3})$. Por tanto,

$$\mathbb{Q}(i\cdot\sqrt{2}, \sqrt[3]{3}) \simeq \mathbb{Q}(i\cdot\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{3}) \simeq \mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{3}) \simeq \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$$

que no es de Galois.

$\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ es el cuerpo de descomposición de $x^3 - 2$, luego es de Galois. Es una $\mathbb{Q}$-extensión de grado 6 y su grupo de Galois es un subgrupo de las permutaciones de las raíces de $x^3 - 2$, luego es isomorfo a S_3.

Problema 8. El polinomio $x^4 - 4 = (x^2-2)(x^2+2)$, luego su cuerpo de descomposición es $\mathbb{Q}(\sqrt{2}, \sqrt{-2}) = \mathbb{Q}(\sqrt{2}, i)$, que es una $\mathbb{Q}$-extensión de grado 4, y el grupo de Galois es isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

El cuerpo de descomposición de $(x^2-2)(x^2+1)$ es $\mathbb{Q}(\sqrt{2}, i)$.

Problema 9. Obvio.

Problema 10. $L = k(\alpha_1, \ldots, \alpha_r)$. Si $p_i(x)$ son los polinomios mínimo anuladores de los α_i, entonces L es el cuerpo de descomposición de $p(x) = p_1(x)\cdots p_r(x)$.

Problema 11. $\mathbb{Q}(\sqrt[n]{2}) = \mathbb{Q}[x]/(x^n - 2)$ es una $\mathbb{Q}$-extensión de grado n. La asignación $\mathrm{Aut}_{\mathbb{Q}-alg}\,\mathbb{Q}(\sqrt[n]{2}) \to \{$ Raíces de $x^n - 2\} \cap \mathbb{Q}(\sqrt[n]{2})$, $\tau \mapsto \tau(\sqrt[n]{2})$ es biyectiva y

$$\{\text{Raíces de } x^n - 2\} \cap \mathbb{Q}(\sqrt[n]{2}) = \begin{cases} \sqrt[n]{2}, & \text{si } n \text{ es impar} \\ \pm\sqrt[n]{2}, & \text{si } n \text{ es par} \end{cases}$$

Por tanto, $\mathbb{Q}(\sqrt[n]{2})$ es una $\mathbb{Q}$-extensión de Galois si y sólo si $n = 1, 2$.

$\mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{Q}(\sqrt[4]{2})$ es una $\mathbb{Q}$-extensión de Galois de grado 2, separable, luego de Galois.

Problema 12. $1/\sqrt{2} + 1/\sqrt{2}i$ es una raíz octava primitiva de la unidad. Luego, $\mathbb{Q}(\sqrt[8]{2}, i)$ es el cuerpo de descomposición de $x^8 - 2$, luego es de Galois de grado 16. Por tanto, el morfismo

$$\mathbb{Z}/8\mathbb{Z} \ltimes \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}_{\mathbb{Q}-alg}\,\mathbb{Q}(\sqrt[8]{2}, i),\ (\bar{r}, \bar{s}) \mapsto \tau_{(\bar{r},\bar{s})},\ \text{ donde } \tau_{(\bar{r},\bar{s})}(\sqrt[8]{2}) = e^{r2\pi i/8}\cdot\sqrt[8]{2},\ \tau_{(\bar{r},\bar{s})}(i) = (-1)^s\cdot i$$

es un isomorfismo. (Consideramos el morfismo de grupos $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}_{grp}(\mathbb{Z}/8\mathbb{Z})$, $\bar{s} \to h_{\bar{s}}$, con $h_{\bar{s}}(\bar{n}) = 3^s\cdot\bar{n}$).

Problema 13. El agujero de L y L' en el cierre algebraico de k, $\bar{k}$ es único. Por tanto, El agujero de $L\cdot L'$ en $\bar{k}$ es único, exactamente es el subcuerpo de $\bar{k}$ generado por L y L'. Por tanto, $L\cdot L'$ (que es separable) es de Galois y todo compuesto de L y L' es isomorfo al subcuerpo de $\bar{k}$ generado por L y L'. $L \otimes_k L'$ (que es separable) es producto directo de compuestos de L y L'.

Problema 14. $(L \otimes_k L') \otimes_k (L \otimes_k L') = (L \otimes_k L) \otimes_k (L' \otimes_k L') = (\prod^n L) \otimes_k (\prod^m L') = \prod^{nm}(L \otimes_k L')$, luego $L \otimes_k L'$ es de Galois. Tenemos el morfismo natural inyectivo

$$G \times G' \to \mathrm{Aut}_k(L \otimes_k L'),\ (g, g') \mapsto g \otimes g'$$

Por órdenes de los grupos, concluimos que es biyectivo.

Problema 15. $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ es el cuerpo de descomposición de $x^3 - 2$, que es una $\mathbb{Q}$-extensión de Galois de grado 6. Sea τ la conjugación compleja. Tenemos que $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})^{\langle\tau\rangle} = \mathbb{Q}(\sqrt[3]{2})$. Si $\sqrt{2} \in \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ entonces $\sqrt{2} \in \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})^{\langle\tau\rangle} = \mathbb{Q}(\sqrt[3]{2})$, lo cual es imposible. Por tanto,

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, e^{2\pi i/3}) = \mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$$

que es una $\mathbb{Q}$-extensión de Galois de grado 12 y grupo $G = \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z} \ltimes \mathbb{Z}/2\mathbb{Z})$. Explícitamente, si denotamos $\tau_{\bar{i},\bar{j},\bar{k}} = (\bar{i}, \bar{j}, \bar{k}) \in \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z} \ltimes \mathbb{Z}/2\mathbb{Z})$, tenemos que

$$\begin{aligned}
\tau_{\bar{i},\bar{j},\bar{k}}(\sqrt{2}) &= (-1)^i \cdot \sqrt{2} \\
\tau_{\bar{i},\bar{j},\bar{k}}(\sqrt[3]{2}) &= (-1)^j \cdot \sqrt[3]{2} \\
\tau_{\bar{i},\bar{j},\bar{k}}(e^{2\pi i/3}) &= e^{k\cdot 2\pi i/3}
\end{aligned}$$

El subgrupo de G que deja invariante a $\sqrt{2} + \sqrt[3]{2}$ es $H = 0 \times 0 \times \mathbb{Z}/2\mathbb{Z}$. Por tanto, $\mathbb{Q}((\sqrt{2} + \sqrt[3]{2}) = \mathbb{Q}((\sqrt{2}, \sqrt[3]{2})$. $\mathbb{Q}((\sqrt{2}, \sqrt[3]{2})$ es una $\mathbb{Q}$-extensión de grado 6, que no es Galois, porque $e^{2\pi i/3} \cdot \sqrt[3]{2} \notin \mathbb{Q}((\sqrt{2}, \sqrt[3]{2})$. Por tanto, su envolvente de Galois es $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, e^{2\pi i/3})$.

Problema 16. El grupo de Galois de $(x^3 + 3)(x^2 + 3)$ es el grupo de Galois de $\mathbb{Q}(\sqrt[3]{3}, e^{2\pi i/3}, \sqrt{3}) = \mathbb{Q}(\sqrt[3]{3}, \sqrt{3}, i)$, que es una $\mathbb{Q}$-extensión de grado 12. El grupo de Galois de $(x^3 + 3)(x^2 + 3)$ es $S_3 \times S_2$.

Problema 17. El grupo de Galois G de una cúbica es un subgrupo del grupo S_3, de permutaciones de las tres raíces $\{\alpha_1, \alpha_2, \alpha_3\}$ de la cúbica. Si la raíz cuadrada del discriminante, $\delta = (\alpha_1 - \alpha_2) \cdot (\alpha_1 - \alpha_3) \cdot (\alpha_2 - \alpha_3) \in k$, entonces G no contiene permutaciones impares, es decir, $G \subseteq A_3$, porque si $g \in G$ es impar entonces $g(\delta) = -\delta$ y $\delta \notin k = k(\alpha_1, \alpha_2, \alpha_3)^G$. Por tanto, $G = A_3$ o $G = \{\mathrm{Id}\}$.

Problema 18. El grupo de Galois de $x^3 - x + 1$ es A_3 ó $\{\mathrm{Id}\}$, por el problema 17. Si es $\{\mathrm{Id}\}$, entonces el cuerpo de descomposición es K y las tres raíces están en K. Si es A_3, entonces el polinomio mínimo anulador de cualquiera de las raíces es $x^3 - x + 1$ y el polinomio es irreducible.

Problema 19. Si tuviése alguna raíz compleja, entonces el automorfismo conjugar sería distinto del morfismo identidad, y como pertenece a A_3 sería de orden 3, lo cual es imposible, pues su orden es 2.

Problema 20. Si el discriminante es positivo, entonces es un cuadrado en $\mathbb{R}$, luego su grupo de Galois es A_3 o $\{\mathrm{Id}\}$. Si alguna raíz fuese compleja, entonces el automorfismo conjugar (en el cuerpo de descomposición de la cúbica) sería distinto de la identidad y de orden 2, lo cual es imposible. Si el discriminante es negativo, el entonces el automorfismo conjugar (en el cuerpo de descomposición de la cúbica) sería distinto de la identidad, luego una raíz con su conjugada son imaginarias y la tercera real.

Problema 21. El grupo de Galois de la cúbica sobre $\mathbb{Q}(\sqrt{\Delta})$ es A_3 o $\{\mathrm{Id}\}$, luego el cuerpo descomposición sobre $\mathbb{Q}(\sqrt{\Delta})$ es igual a $\mathbb{Q}(\sqrt{\Delta})(\alpha)$. Por tanto, el cuerpo de descomposición de la cúbica sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{\Delta}, \alpha)$.

Problema 22. Sea ε_3 una raíz cúbica primitiva de la unidad. El cuerpo de descomposición de $x^3 - a$ es $k(\sqrt[3]{a}, \varepsilon_3)$. Si $\varepsilon_3 \in k$, entonces el cuerpo de descomposición es $k(\sqrt[3]{a})$ y el grupo de Galois es $\mathbb{Z}/3\mathbb{Z}$, si $\sqrt[3]{a} \notin k$ ó $\{\mathrm{Id}\}$ si $\sqrt[3]{a} \in k$. Si $\varepsilon_3 \notin k$, entonces el cuerpo de composición es la cúbica es de grado 6, si $\sqrt[3]{a} \notin k$, luego su grupo de Galois es S_3, ó el cuerpo de descomposición es $k(\varepsilon_3)$, si $\sqrt[3]{a} \in k$, luego su grupo de Galois es $\mathbb{Z}/2\mathbb{Z}$.

Problema 23. Por el problema 22, el grupo de Galois sobre $\mathbb{Q}(a)$ es S_3 y sobre $\mathbb{C}(a)$ es $\mathbb{Z}/3\mathbb{Z}$.

Problema 24. Considérese la sección de s, $L^H \hookrightarrow L$, $l \mapsto \frac{1}{\#H} \cdot l$.

Problema 25. El cuerpo de descomposición de x^3-2 es $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3} \cdot \sqrt[3]{2}, e^{4\pi i/3} \cdot \sqrt[3]{2})$, de grupo de Galois S_3. Los subgrupos de S_3, son $S_3, \langle(1,2,3)\rangle, \langle(1,2)\rangle, \langle(1,3)\rangle, \langle(2,3)\rangle$ y $\{\mathrm{Id}\}$, que por toma de invariantes se corresponden con las subextensiones

$$\mathbb{Q},\ \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{3} \cdot i),\ \mathbb{Q}(e^{4\pi i/3} \cdot \sqrt[3]{2}),\ \mathbb{Q}(e^{2\pi i/3} \cdot \sqrt[3]{2}),\ \mathbb{Q}(\sqrt[3]{2}),\ \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$$

El cuerpo de descomposición de $(x^2-2)(x^2+1)$ es $\mathbb{Q}(\sqrt{2}, i)$ de grupo de Galois $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/frm-e\mathbb{Z}$. Los subgrupos son $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/frm-e\mathbb{Z}$, $\langle(\bar{1},\bar{0})\rangle$, $\langle(\bar{0},\bar{1})\rangle$, $\langle(\bar{1},\bar{1})\rangle$, $\{\mathrm{Id}\}$, que por toma de invariantes se corresponden con las subextensiones

$$\mathbb{Q},\ \mathbb{Q}(i),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{2} \cdot i),\ \mathbb{Q}(\sqrt{2}, i)$$

El cuerpo de descomposición de x^4-4 es $\mathbb{Q}(\sqrt{2}, i)$.

Problema 26. $\sqrt{3} \notin \mathbb{Q}(\sqrt[4]{2})$ (compruébese).

Por tanto, $\mathbb{Q}(\sqrt{3}, \sqrt[4]{2})$ es una $\mathbb{Q}$-extensión de grado 8. Como $i \notin \mathbb{Q}(\sqrt{3}, \sqrt[4]{2})$, $\mathbb{Q}(\sqrt{3}, \sqrt[4]{2}, i)$ es una $\mathbb{Q}$-extensión de grado 16, luego una $\mathbb{Q}(\sqrt{3})$-extensión de grado 8. Por tanto, $\dim_{\mathbb{Q}(\sqrt{3})} \mathbb{Q}(\sqrt{3}, \sqrt[4]{2}) = 4$ y x^4-2 es irreducible sobre $\mathbb{Q}(\sqrt{3})$.

Problema 27. $L_1 = L^{\mathbb{Z}/2\mathbb{Z}\times 0}$ y $L_2 = L^{0\times\mathbb{Z}/2\mathbb{Z}}$ son dos $\mathbb{Q}$-subextensiones de grado 2 (de Galois). Luego, $L_1 = \mathbb{Q}(\alpha)$, con $\alpha^2 \in \mathbb{Q}$, y $L_2 = \mathbb{Q}(\beta)$, con $\beta^2 \in \mathbb{Q}$. Por último,

$$L = L^{(\mathbb{Z}/2\mathbb{Z}\times 0)\cap(0\times\mathbb{Z}/2\mathbb{Z})} = L_1 \cdot L_2 = \mathbb{Q}(\alpha, \beta)$$

Problema 28. Sea L' la envolvente de Galois de L. Las subextensiones de L' son un número finito, porque se corresponden con los subgrupos del grupo de Galois de L'. Por tanto, las subextensiones de L, que son subextensiones de L', son un número finito.

Problema 29. Si las subextensiones $k(\alpha + a\beta)$ son todas distintas variando $a \in k$, tendríamos que el número de subextensiones de $k(\alpha, \beta)$ sería infinito, lo que contradice el problema 28. Por tanto, existen $a \neq b \in k$ tales que $k(\alpha + a\beta) = k(\alpha + b\beta)$. Luego, $(\alpha + a\beta) - (\alpha + b\beta) \in k(\alpha + a\beta)$, $\beta \in k(\alpha + a\beta)$, $\alpha \in k(\alpha + a\beta)$ y $k(\alpha + a\beta) = k(\alpha, \beta)$.

Problema 30. $L \otimes_k L$ es una L-extensión separable de grado 2, con un punto L-racional. Por tanto, $L \otimes_k L = L \times L'$ y por grados $L' = L$. En conclusión, L es de Galois.

Toda extensión de cuerpos de grado n, con n primo con la característica es separable, pues todo el grado del polinomio mínimo anulador de todo elemento divide a n, luego su derivada es no nula y el polinomio (irreducible) es separable. Por tanto, toda extensión de cuerpos de grado dos es de Galois, en característica distinta de 2. En característica dos $\mathbb{F}_2(x) \hookrightarrow \mathbb{F}_2(\sqrt{x})$ no es separable, pero $\mathbb{F}_2(x) \hookrightarrow \mathbb{F}_2(x)[y]/(y^2+y+x)$ es separable, luego de Galois.

Problema 31. $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{Q}(\sqrt[4]{2})$ son extensiones de Galois, pero $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt[4]{2})$ no es de Galois, pues $i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$.

Problema 32. $\sigma^2(\varepsilon_5) = \varepsilon_5^{16} = \varepsilon_5$, luego $\sigma^2 = \mathrm{Id}$. Por tanto, $H = \langle\sigma\rangle$ es un grupo de orden 2. Como $\mathbb{Q} \hookrightarrow \mathbb{Q}(\varepsilon_5)$ es una extensión de Galois de grado 4, entonces $\mathbb{Q}(\varepsilon_5)^H$ es una $\mathbb{Q}$-extensión de grado 2. Como $\frac{-1+\sqrt{5}}{2} = \varepsilon_5 + \varepsilon_5^4 \in \mathbb{Q}(\varepsilon_5)^H$, entonces $\sqrt{5} \in \mathbb{Q}(\varepsilon_5)^H$ y $\mathbb{Q}(\varepsilon_5)^H = \mathbb{Q}(\sqrt{5})$.

Problema 33. El cuerpo de descomposición de $x^6 - 8$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{2}, e^{2\pi i/3}) = \mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/3})$, que es una $\mathbb{Q}$-extensión de grado 4, de grupo de Galois $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Sobre $\mathbb{Q}(\sqrt{2})$ es $\mathbb{Z}/2\mathbb{Z}$ y sobre $\mathbb{Q}(e^{2\pi i/3})$ es $\mathbb{Z}/2\mathbb{Z}$. $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}, e^{2\pi i/3})$ es una $\mathbb{Q}$-extensión de grado $3 \cdot 4 = 12$, luego es una $\mathbb{Q}(\sqrt[3]{2}$-extensión de Galois de grado 4, de grupo de Galois $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $\mathbb{Q}(\sqrt[4]{2}, \sqrt{2}, e^{2\pi i/3}) = \mathbb{Q}(\sqrt[4]{2}, e^{2\pi i/3})$ es una $\mathbb{Q}$-extensión de grado $4 \cdot 2 = 8$, luego es una $\mathbb{Q}(\sqrt[4]{2}$-extensión de Galois de grado 2, de grupo de Galois $\mathbb{Z}/2\mathbb{Z}$.

Problema 34. El grupo de Galois de $\mathbb{Q}(e^{2\pi i/8})$ sobre $\mathbb{Q}$ es $(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, que son todos de grado dos salvo la identidad. Luego $\langle\tau\rangle$ es de orden 2, salvo $\tau = \mathrm{Id}$. Luego, el grado de $\mathbb{Q}(\varepsilon_8)^\tau$ es $4/2 = 2$, salvo para $\tau = \mathrm{Id}$, que 4.

No hay ningún automorfismo de $\mathbb{Q}(\varepsilon_8)$ que sólo deje fijos los números racionales.

Problema 35. El grupo de Galois de $\mathbb{Q}(e^{2\pi i/n})$ es $(\mathbb{Z}/n\mathbb{Z})^*$. Para $n = 3$, es $\mathbb{Z}/2\mathbb{Z}$ que contiene un único subgrupo de índice dos. Para $n = 5$ es $\mathbb{Z}/4\mathbb{Z}$, que contiene un único subgrupo de índice dos. Para $n = 6$, es $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^* = (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/2\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z}$ que contiene un único subgrupo de índice dos. Para $n = 7$ es $\mathbb{Z}/6\mathbb{Z}$, que contiene un único subgrupo de índice dos. Para $n = 8$, es $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ que contiene tres subgrupos de índice dos. Para $n = 9$, es $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}$ que contiene un único subgrupo de índice dos. Para $n = 10$, es $\mathbb{Z}/4\mathbb{Z}$ que contiene un único subgrupo de índice dos. Para $n = 11$ es $\mathbb{Z}/10\mathbb{Z}$, que contiene un único subgrupo de índice dos. Para $n = 12$, es $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/4\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ que contiene tres subgrupos de índice dos. Para $n = 13$ es $\mathbb{Z}/12\mathbb{Z}$, que contiene un único subgrupo de índice 2.

Problema 36. Para $n = 5$, el grupo de Galois es $(\mathbb{Z}/5\mathbb{Z})^* \simeq \mathbb{Z}/4\mathbb{Z}$, que tiene un único subgrupo propio, $H = \langle\bar{4}\rangle = \langle\tau\rangle$, donde τ es el automorfismo conjugar. Entonces, $\mathbb{Q}(e^{2\pi i/5})^H = \mathbb{Q}(e^{2\pi i/5} + e^{-2\pi i/5}) = \mathbb{Q}(\sqrt{5})$. Para $n = 6$, el grupo de Galois es $\mathbb{Z}/2\mathbb{Z}$, que no tiene subgrupos propios. Para $n = 7$, el grupo de Galois es $(\mathbb{Z}/7\mathbb{Z})^* \simeq \mathbb{Z}/6\mathbb{Z}$, que contiene dos subgrupos propios, $H_1 = \langle\bar{2}\rangle \simeq \mathbb{Z}/3\mathbb{Z}$ y $H_2 = \langle\bar{6}\rangle \simeq \mathbb{Z}/2\mathbb{Z}$. $\mathbb{Q}(e^{2\pi i/7})^{H_1} = \mathbb{Q}(e^{2\pi i/7} + e^{4\pi i/7} + e^{8\pi i/7})$, porque si $e^{2\pi i/7} + e^{4\pi i/7} + e^{8\pi i/7} = a \in \mathbb{Q}$, entonces $x + x^2 + x^4 - a$ anularía a $e^{2\pi i/7}$ (además, si denotamos $w = e^{2\pi i/7} + e^{4\pi i/7} + e^{8\pi i/7}$, entonces su polinomio anulador resulta ser $x^2 + x + 2$, luego $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{-7})$. $\mathbb{Q}(e^{2\pi i/7})^{H_2} = \mathbb{Q}(e^{2\pi i/7} + e^{-2\pi i/7})$. Para $n = 8$, el grupo de Galois es $(\mathbb{Z}/8\mathbb{Z})^* = \langle\bar{1}, \bar{3}, \bar{5}, \bar{7}\rangle = \langle\bar{1}, \bar{3}\rangle \times \langle\bar{1}, \bar{5}\rangle = H_1 \times H_2$. $\mathbb{Q}(e^{2\pi i/8})^{H_2} = \mathbb{Q}(e^{\pi i/2}) = \mathbb{Q}(i)$ y $\mathbb{Q}(e^{2\pi i/8})^{H_1} = \mathbb{Q}(e^{2\pi i/8} + e^{6\pi i/8})$, (además, si denotamos $w = e^{2\pi i/8} + e^{6\pi i/8}$, entonces su polinomio anulador resulta ser $x^2 + 2$, luego $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{-2})$). $H_1 \times H_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ contiene tres subgrupos propios (de orden 2), nos falta considerar la subextensión $\mathbb{Q}(\sqrt{-2} \cdot i) = \mathbb{Q}(\sqrt{2})$. Para $n = 9$, el grupo de Galois es $(\mathbb{Z}/9\mathbb{Z})^* = \langle\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\rangle = \langle\bar{8}\rangle \times \langle\bar{4}\rangle = H_1 \times H_2$. $\mathbb{Q}(e^{2\pi i/9})^{H_1} = \mathbb{Q}(e^{2\pi i/9} + e^{-2\pi i/9})$ y $\mathbb{Q}(e^{2\pi i/9})^{H_2} = \mathbb{Q}(e^{6\pi i/9}) = \mathbb{Q}(e^{2\pi i/3}) = \mathbb{Q}(\sqrt{-3})$.

Problema 37. Supongamos que $\sqrt{b} \notin \mathbb{Q}$ (es decir, que b no es el cuadrado de un número racional). Entonces, $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{b})$ es una extensión de grado 2. Para $n = 5$, $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{5})$, luego $\sqrt{b} = a_1 + a_2\sqrt{5}$, con $a_1, a_2 \in \mathbb{Q}$. Elevando al cuadrado, observamos que $a_1 = 0$ y que $b = a_2^2 \cdot 5$. Para $n = 6$, nunca. Para $n = 7$, $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{-7})$, luego $b = -a_2^2 \cdot 7$. Para $n = 8$, $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{-1})$, luego $b = -a_2^2$; ó $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{-2})$, luego $b = -2 \cdot a_2^2$; ó $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{2})$, luego $b = 2 \cdot a_2^2$. Para $n = 9$, $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{-3})$, luego $b = -3 \cdot a_2^2$.

Problema 38. a. Por el teorema de equivalencia de Galois, tenemos que demostrar que $\mathbb{Z}/n\mathbb{Z}$ sólo contiene para cada divisor d' de n un único subgrupo de orden d'. En efecto, el subgrupo es cíclico, luego está generado por un elemento de orden d'. Los elementos de $\mathbb{Z}/n\mathbb{Z}$ anulados por d', son $\overline{n/d'}$, $2 \cdot \overline{n/d'}, \cdots, (d'-1) \cdot \overline{n/d'}$,

los cuales forman un subgrupo de orden d'. En conclusión, $\langle \overline{n/d'} \rangle$ es el único subgrupo de orden d' de $\mathbb{Z}/n\mathbb{Z}$.

b. Por el teorema de equivalencia de Galois, tenemos que demostrar que si tenemos dos subgrupos $H_1 = \langle \bar{r} \rangle$,$H_2 = \langle \bar{s} \rangle$ de $\mathbb{Z}/n\mathbb{Z}$ (con r y s divisores de n), entonces $H_1 \subseteq H_2$ si y sólo si $\#H_1 | \#H_2$. Ahora bien, $H_1 \subseteq H_2$ si y sólo si s divide a r, que equivale a decir que $n/r = \#H_1$ divide a $n/s = \#H_2$.

Problema 39. $\mathbb{Q}(\sqrt{-2}, i)$ es una extensión de Galois de grupo $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ que contiene exactamente tres subgrupos de índice 2. Luego, $\mathbb{Q}(\sqrt{-2}, i)$ contiene tres subextensiones de grado 2: $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(i)$ y $\mathbb{Q}(\sqrt{-2}\cdot i) = \mathbb{Q}(\sqrt{2})$. Ninguna de estas tres contiene a $\sqrt{-3}$.

Problema 40. $L = \mathbb{Q}(\sqrt{3}, \sqrt{2}, i)$ es una extensión de Galois de grupo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Todos los elementos de este grupo son de orden 2, salvo el elemento neutro, luego contiene 7 subgrupos de orden 2. El elemento $\sigma = (\bar{r}, \bar{s}, \bar{t}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, opere como sigue $\sigma(\sqrt{3}) := (-1)^r \cdot \sqrt{3}$, $\sigma(\sqrt{2}) = (-1)^s \cdot \sqrt{2}$, $\sigma(i) = (-1)^t \cdot i$. Si L' es real entonces es invariante por $H = 0 \times 0 \times \mathbb{Z}/2\mathbb{Z}$ y $L^H = \mathbb{Q}(\sqrt{3}, \sqrt{2})$, luego $L' = \mathbb{Q}(\sqrt{3}, \sqrt{2})$. $\mathbb{Q}(\sqrt[4]{3})$ es una $\mathbb{Q}$-extensión de grado 4, que no es de Galois, luego no coincide con $\mathbb{Q}(\sqrt{3}, \sqrt{2})$, por tanto, $\sqrt[4]{3} \notin L' = L \cap \mathbb{R}$ y $\sqrt[4]{3} \notin L$. Entonces, $L \hookrightarrow L(\sqrt[4]{3}) = \mathbb{Q}(\sqrt[4]{3}, \sqrt{2}, i)$ es de grado 2, luego $\mathbb{Q}(\sqrt[4]{3}, \sqrt{2}, i)$ es una $\mathbb{Q}$-extensión de grado 16. Además es es el compuesto de dos extensiones de Galois: $\mathbb{Q}(\sqrt[4]{3}, i)$ y $\mathbb{Q}(\sqrt{2})$, luego es de Galois.

Problema 41. El grupo de Galois de L es $(\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$: $\sigma = (\bar{r}, \bar{s}, \bar{t}) \in (\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$ opera como sigue $\sigma(\sqrt[4]{3}) = i^r \cdot \sqrt[4]{3}$, $\sigma(i) = (-1)^s \cdot i$ y $\sigma(\sqrt{2}) = (-1)^t \cdot \sqrt{2}$. Puede comprobarse que $(\bar{r}, \bar{s}, \bar{t}) + (\bar{r}, \bar{s}, \bar{t}) = (\bar{r} + (-1)^s \cdot \bar{r}, 0, 0)$, que es cero si $s = 1$, ó $s = 0$ y $r = 0, 2$. En total, 11 subgrupos de orden 2. Si L' es de real, entonces es invariante por $H = 0 \times \mathbb{Z}/2\mathbb{Z} \times 0$ y $L' \subseteq L^H = \mathbb{Q}(\sqrt[4]{3}, \sqrt{2})$.

Si $\sqrt[8]{3} \in L$ entonces $L = \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$. Observemos que $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(e^{2\pi i/8})$. El grupo de Galois, G, de la extensión de Galois de grado 4, $\mathbb{Q}(\sqrt{2}, i) \to L = \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$ es $\mathbb{Z}/4\mathbb{Z}$, pues es un subgrupo de $\mathbb{Z}/8\mathbb{Z}$, pues dado $\tau \in G$, $\tau(\sqrt[8]{3}) = e^{r\cdot 2\pi i/8} \cdot \sqrt[8]{3}$, para cierto $\bar{r} \in \mathbb{Z}/8\mathbb{Z}$ (y $\tau^m((\sqrt[8]{3}) = e^{mr\cdot 2\pi i/8} \cdot \sqrt[8]{3})$. Por tanto, $G = \langle \sigma \rangle$, con $\sigma(\sqrt[8]{3}) = e^{2\pi i/4} \cdot \sqrt[8]{3}$ y el polinomio mínimo anulador de $\sqrt[8]{3}$ es $x^4 - \sqrt{3}$. Por tanto, $\sqrt{3} \in \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(e^{2\pi i/8})$, lo cual es falso, por el problema 37.

Problema 42. $\mathbb{Q}(\sqrt[8]{3}, i)$ fuese una $\mathbb{Q}$-extensión de Galois, entonces contendría todas las raíces de $x^8 - 3$, luego contendría a $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(e^{2\pi i/8})$. Por tanto, $\mathbb{Q}(\sqrt[8]{3}, i) = \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$ y llegamos a contradicción con el problema 41.

Problema 43. Las raíces de $x^4 + 2$ son

$$\sqrt[4]{-2} = \sqrt[4]{2} \cdot \sqrt[4]{-1} = \begin{cases} \pm\sqrt[4]{2} \cdot (\sqrt{2}/2 + \sqrt{2}2i) = \pm(1/\sqrt[4]{2} + 1/\sqrt[4]{2} \cdot i) \\ \pm i \cdot (1/\sqrt[4]{2} + 1/\sqrt[4]{2} \cdot i) \end{cases}$$

Si $i \in \mathbb{Q}(\alpha)$, entonces $\mathbb{Q}(\alpha)$ es el cuerpo de descomposición de $x^4 + 2$, que coincide con $\mathbb{Q}(\sqrt[4]{2}, i)$ que es de grado 8 sobre $\mathbb{Q}$, lo cual es contradictorio. Observemos que $\sqrt{-2} \in \mathbb{Q}(\alpha)$, luego si $\sqrt{2} \in \mathbb{Q}(\alpha)$ entonces $i \in \mathbb{Q}(\alpha)$ y hemos probado que no es así.

El grupo de Galois de $\mathbb{Q}(\sqrt[4]{2}, i)$ es $G = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ y los inavariantes por $H = \langle (\bar{1}, \bar{1}) \rangle$ es $\mathbb{Q}(\alpha)$. Las extensiones de grado 2 son de Galois. Buscamos subgrupos H' de orden 4 de G, normales que contengan a H. Por ser normal ha de contener a $(-\bar{1}, \bar{1}) = (0, \bar{1}) * (\bar{1}, \bar{1}) * (0, \bar{1})^{-1}$. Luego $H' = \langle (\bar{1}, \bar{1}), (-\bar{1}, \bar{1}) \rangle$ y solo hay una subextensión de grado 2: $\mathbb{Q}(\sqrt{-2})$.

Problema 44. El polinomio mínimo anulador de $\sqrt{2+\sqrt{2}}$ es $x^4 - 4x^2 + 2$, pues anula y es irreducible por el criterio de Eisenstein. Sus raíces son $\pm\sqrt{2\pm\sqrt{2}}$. $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ es una extensión de Galois de $\mathbb{Q}$ si y sólo si $\beta = \sqrt{2-\sqrt{2}} \in \mathbb{Q}(\alpha = \sqrt{2+\sqrt{2}})$. Ahora bien, $\alpha \cdot \beta = \sqrt{2}$, luego $\beta = \sqrt{2}/\alpha \in \mathbb{Q}(\alpha)$.

De otro modo: el grupo de Galois de esta bicuadrada se puede calcular y es de orden 4.

Problema 45. Consideremos la extensión de Galois $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, cuyo grupo de Galois es $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. El polinomio $(x^2-2)\cdot(x^2-3)\cdot(x^2-6)$ cumple lo requerido.

Problema 46. Sea $g \in G - (H_1 \cup \ldots \cup H_n)$. Por definición g no deja fija ninguna raíz.

Problema 47. El cuerpo formado por las raíces es finito. Por tanto, es de característica positiva p. Luego, el cuerpo es de orden p^n, y $x^{p^n} - x$ tiene justamente como raíces los elementos del cuerpo y ha de coincidir con $q(x)$.

Problema 48. Sea α una raíz del polinomio irreducible $y^2 - y + 1$. Veamos que $\sqrt{\alpha} \in \mathbb{F}_5(\alpha)$: Calculemos $a, b \in \mathbb{F}_5$ tales que $(a + b\alpha)^2 = \alpha$. En tal caso, $a^2 + b^2\alpha^2 + 2ab\alpha - \alpha = 0$, luego $0 = a^2 + b^2(\alpha - 1) + 2ab\alpha - \alpha = (a^2 + b^2) + (b^2 + 2ab - 1)\alpha = 0$. Por tanto, $a^2 - b^2 = 0$ y $b^2 + 2ab - 1 = 0$. Una solución es $a = 2$ y $b = -2$. Entonces el cuerpo de descomposición de $x^4 - x^2 + 1$ es $\mathbb{F}_5(\alpha)$, cuyo grupo de Galois (que está generado por el automorfismo de Frobenius) es $\mathbb{Z}/5\mathbb{Z}$.

Las raíces de $y^2 - y + 1$ son $2 \pm 3\sqrt{2}$ y las de $x^4 - x^2 + 1$, $\pm(2 - 2(2 \pm 3\sqrt{2})) = \pm(3 + \mp\sqrt{2})$.

Problema 49. Sea $\mathbb{F}_{25}$ el único cuerpo con 25 elementos, cuyos elementos son las raíces de $x^{25} - x$. Dado un polinomio, $p(x)$ de grado 2 irreducible, entonces $\mathbb{F}_5[x]/(p(x)) = \mathbb{F}_{25}$. Luego las raíces de $p(x)$ están en $\mathbb{F}_{25}$. Recíprocamente, dada $\alpha \in \mathbb{F}_{25} - \mathbb{F}_5$, su polinomio mínimo anulador es de grado 2. En conclusión, las raíces de todos los polinomios mónicos e irreducibles de grado ≤ 2 con coeficientes en $\mathbb{F}_5$ coinciden con los elementos de $\mathbb{F}_{25}$, luego el producto de todos los polinomios mónicos e irreducibles de grado ≤ 2 con coeficientes en $\mathbb{F}_5$ tiene las mismas raíces que $x^{25} - x$, luego son iguales.

Problema 50. Si $p(x)$ es un polinomio irreducible de grado 2 con coeficientes en $\mathbb{F}_p$, entonces $\mathbb{F}_p[x]/(p(x))$ es un cuerpo con p^2 elementos, luego $\mathbb{F}_p[x]/(p(x)) = \mathbb{F}_{p^2}$, luego las raíces de $p(x)$ pertenecen a $\mathbb{F}_{p^2}$. Dado $\alpha \in \mathbb{F}_{p^2}$, tenemos $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^2}$, luego el grado de $\mathbb{F}_p(\alpha)$ sobre $\mathbb{F}_p$ es 1 ó 2. Es decir, α es raíz de un polinomio irreducible de grado 1 ó 2. Es decir, $\mathbb{F}_{p^2} - \mathbb{F}_p$ son todos los elementos de polinomio anulador de grado 2 y cada uno de estos polinomios tiene dos raíces, luego el número de polinomios irreducibles de grado 2 es igual a

$$\#(\mathbb{F}_{p^2} - \mathbb{F}_p)/2 = (p^2 - p)/2$$

Si $\{p_i(x)\}_{i\in I}$ es el conjunto de los polinomios mónicos irreducibles de grado 2, entonces $\{a \cdot p_i(x)\}_{i\in I, a\in\mathbb{F}_p^*}$ es el conjunto de los polinomios irreducibles de grado 2. Por tanto, el número de polinomios mónicos irreducibles de grado 2 con coeficientes en $\mathbb{F}_p$ es $(p_1)\cdot(p^2 - p)/2 = p(p-1)^2/2$.

Problema 51. Los elementos de polinomio mínimo anulador de grado 3 son los elementos de $\mathbb{F}_{p^3} - \mathbb{F}_p$ ($\mathbb{F}_{p^3}$ no contiene subextensiones propias). Luego el número de los polinomios mónicos irreducibles de grado 3 con coeficientes en $\mathbb{F}_p$ es igual a

$$\#(\mathbb{F}_{p^3} - \mathbb{F}_p)/3 = (p^3 - p)/3$$

Los elementos de polinomio mínimo anulador de grado 4 son los elementos de $\mathbb{F}_{p^4} - \mathbb{F}_{p^2}$ ($\mathbb{F}_{p^2}$ el la única subextensión propia de $\mathbb{F}_{p^4}$). Luego el número de los polinomios mónicos irreducibles de grado 4 con coeficientes en $\mathbb{F}_p$ es igual a

$$\#(\mathbb{F}_{p^4} - \mathbb{F}_{p^2})/4 = (p^4 - p^2)/4$$

Los elementos de polinomio mínimo anulador de grado 6 son los elementos de $\mathbb{F}_{p^6} - (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})$. Luego el número de los polinomios mónicos irreducibles de grado 6 con coeficientes en $\mathbb{F}_p$ es igual a

$$(\#\mathbb{F}_{p^4} - \#(\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}))/6 = (p^6 - (p^2 + p^3 - p))/6$$

Los elementos de polinomio mínimo anulador de grado 8 son los elementos de $\mathbb{F}_{p^8} - \mathbb{F}_{p^4}$. Luego el número de los polinomios mónicos irreducibles de grado 8 con coeficientes en $\mathbb{F}_p$ es igual a

$$(\#(\mathbb{F}_{p^8} - \#\mathbb{F}_{p^4})/4 = (p^8 - p^4)/8$$

Problema 52. El núcleo del morfismo de grupos $\mathbb{F}_p^* \to \mathbb{F}_p^*$ $\bar{a} \mapsto \bar{a}^2$ lo forman las raíces de $x^2 - 1$, que son ± 1. Por tanto, la imagen de este morfismo, $\mathbb{F}_p^{*2}$, es de orden $(p-1)/2$. Luego, $\mathbb{F}_p^*/\mathbb{F}_p^{*2}$ es un grupo de orden 2, entonces isomorfo a $\{\pm 1\}$. Explícitamente, $\mathbb{F}_p^*/\mathbb{F}_p^{*2} = \{\pm 1\}$, $\bar{a} \mapsto \bar{a}^{(p-1)/2}$.

Problema 53. Por el problema 52, sabemos que p es resto cuadrático módulo q si y sólo si $p^{(q-1)/2} = 1$ en $\mathbb{F}_q^*$, es decir, si y sólo si el orden de p en $\mathbb{F}_q^*$ es $(q-1)/(2d)$, que equivale a decir, que p genera en $\mathbb{F}_q^*$ un subgrupo de índice $2d$.

Problema 54. Tenemos que ver que $\mathbb{F}_p^{*2} \cap \{-\bar{1}, -\bar{2}, \bar{2}\} \neq \emptyset$. En efecto, no puede ser que $(-1)^{(p-1)/2} = (2)^{(p-1)/2} = (-1)^{(p-1)/2} = -1$ en $\mathbb{F}_p^*$, porque el producto de los dos primeros es el tercero.

Problema 55. El grupo multiplicativo $\mathbb{F}_{p^n}^*$ es isomorfo a $\mathbb{Z}/(p^n - 1)$. Por tanto, las raíces q-ésimas de la unidad se identifica con los elementos de $\mathbb{Z}/(p^n - 1)$ anulados por q, que son $\{0\}$ si q es primo con $p^n - 1$, ó $\langle (p^n - 1)/q \rangle$ (que son q elementos) si q divide a $p^n - 1$.

Problema 56. Sea ε_q una raíz de $x^{q-1} + \ldots + x + 1 \in \mathbb{F}_p[x]$, cuyo polinomio mínimo anulador, $q(x)$ lo divide. $\mathbb{Z}/q\mathbb{Z}$ es isomorfo al conjunto de las raíces de $x^q - 1$ y tenemos que

$$\langle F \rangle = \mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_p(\varepsilon_q) \subseteq (\mathbb{Z}/\mathfrak{q}\mathbb{Z})^*,\ F \mapsto \bar{p}$$

Como $\#\,\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_p(\varepsilon_q) = \mathrm{gr}\, q(x)$. Tenemos que $\bar{p}$ genera $(\mathbb{Z}/\mathfrak{q})^*$ si y sólo si $\mathrm{gr}\, q(x) = q - 1$, es decir, si y sólo si $q(x) = x^{q-1} + \ldots + x + 1$, es decir, si y sólo si $x^{q-1} + \ldots + x + 1$ es irreducible.

Problema 57. $\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_p(\sqrt{3}) = \langle F \rangle \subseteq (\mathbb{Z}/12\mathbb{Z})^* = \langle \bar{1}, \bar{5}, \bar{7}, -\bar{1} \rangle$, $F \mapsto \bar{p}$. El polinomio de raíces primitivas 12-ésimas de la unidad es $x^4 - x^2 + 1$. Si hacemos el cambio $y = x + 1/x$, tenemos que $x^4 - x^2 + 1 = x^2(y^2 - 3)$. Por tanto, $\varepsilon_{12} + 1/\varepsilon_{12} = \sqrt{3}$. Por tanto, $\sqrt{3} \in \mathbb{F}_p \iff F(\sqrt{3}) = \sqrt{3} \iff \bar{p} = \pm\bar{1}$.

Problema 58. El discriminante δ del polinomio $x^q - 1$ es igual a $q^{(q-1)/2}\sqrt{-q}$. Entonces, como $\sqrt{-1}, \delta \in \mathbb{F}_p(\varepsilon_{4q})$, tenemos que $\sqrt{q} \in \mathbb{F}_p(\varepsilon_{4q})$.

Problema 59. La sucesión $1 \to \pm 1 \to \mathbb{F}_q^* \to \mathbb{F}_q^{*2} \to 1$ es exacta, luego $\#\mathbb{F}_q^{*2} = (q-1)/2$, luego el número de cuadrados en $\mathbb{F}_q$ es $(q+1)/2$. Por órdenes, Q y $a - Q$ no pueden ser disjuntos, luego existen $b_1, b_2 \in Q$ tales que $a - b_1 = b_2$ y $a = b_1 + b_2$.

Problema 60. $\mathbb{F}_{p^n}^* \simeq \mathbb{Z}/(p^n - 1) = \mathbb{Z}/((p-1)(p^{n-1} + p^{n-2} + \cdots + 1))$. Vía este isomorfismo la norma N es igual a multiplicar por $p + p^2 + \cdots + p^n \equiv p^{n-1} + p^{n-2} + \cdots 1$, luego el orden de la imagen es $p - 1$ y N es epiyectivo.

Problema 61. Si $x^3 + ax - b$ es irreducible en $\mathbb{F}_p[x]$, es decir, $x^3 + ax \equiv b$ (módulo p) no admite alguna solución entera, entonces su grupo de Galois sobre $\mathbb{F}_p$ es $\mathbb{Z}/3\mathbb{Z} = A_3$. En este caso, si $\delta = (\alpha_1 - \alpha_2)\cdot(\alpha_2 - \alpha_3)\cdot(\alpha_2 - \alpha_3) = \sqrt{-4a^3 - 27b^2}$, entonces $\mathbb{F}_p = \mathbb{F}_p(\alpha_1)^{A_3} = \mathbb{F}_p(\sqrt{-4a^3 - 27b^2})$ y llegamos a contradicción.

Problema 62. Entonces, la sucesión

$$1 \to \mathrm{Aut}_{L'-alg}L \to \mathrm{Aut}_{k-alg}L \to \mathrm{Aut}_{k-alg}L' \to 1$$

es exacta y $\#\mathrm{Aut}_{k-alg}L = \#\mathrm{Aut}_{L'-alg}L \cdot \#\mathrm{Aut}_{k-alg}L' = \dim_{L'} L \cdot \dim_k L' = \dim_k L$ y L es una k-extensión de Galois.

Problema 63. Por el teorema de prolongación, todo morfismo de K_1 en K prolonga a automorfismo de K. Sea $i\colon K_2 \hookrightarrow K$ la inclusión. El morfismo $i \circ f$ prolonga al automorfismo σ buscado.

Problema 64. Denotemos $i_1\colon K_1 \hookrightarrow L$, $i_2\colon K_2 \hookrightarrow L$ las inclusiones y $\sigma\colon K_1 \simeq K_2$ el isomorfismo. Consideremos el morfismo $i_2 \circ \sigma L_1 \to L$. Por el teorema de prolongación existe un automorfismo $g\colon L \to L$, tal que $i_2 \circ \sigma = g \circ i_1$. Por tanto, $g(K_1) = K_2$. Entonces, si $K_1 = L^{H_1}$, se tiene que $L^{H_2} := K_2 = g(K_1) = L^{gH_1g^{-1}}$. Luego, $H_2 = gH_1g^{-1}$. Recíprocamente, si $H_2 = gH_1g^{-1}$, entonces $K_2 = g(K_1)$ y $K_2 \simeq K_1$.

Problema 65. Sea $G = \mathrm{Aut}_{k-alg}\, L'$. Dada una extensión $L' \hookrightarrow L$ y $g \in G$, denotemos L_g, la L'-extensión $L' \xrightarrow{g} L' \hookrightarrow L$. En la línea superior si consideramos $L' \otimes_k L$ como L'-álgebra vía el primer factor de $L' \otimes_k L$ y queremos considerar $\oplus L$ como L'-álgebra vía el isomorfismo $L' \otimes_k L = \oplus L$, entonces deberíamos escribir en vez de $\oplus L$, $\oplus_{g\in G} L_g$. Ahora en la línea inferior tendremos $\oplus_{g\in G} L \otimes_{L'} L_g$.

Por ejemplo, si $L' = \mathbb{Q}(\sqrt{2})$ y $L = \mathbb{Q}(\sqrt[4]{2}$, entonces $G = \mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt{2}) = \{\mathrm{Id}, g\}$, con $g(\sqrt{2}) = -\sqrt{2}$. Tenemos el diagrama conmutativo

$$\begin{array}{ccc} \mathbb{Q}(i\cdot\sqrt[4]{2}) & \xrightarrow{\sim} & \mathbb{Q}(\sqrt[4]{2}) \\ \uparrow & & \uparrow \\ \mathbb{Q}(\sqrt{2}) & \xrightarrow[g]{\sim} & \mathbb{Q}(\sqrt{2}) \end{array} \qquad \begin{array}{c} i\cdot\sqrt[4]{2} \longmapsto \sqrt[4]{2} \\ \\ \sqrt{2} \longmapsto -\sqrt{2} \end{array}$$

Luego, $L \otimes_{L'} L_g = \mathbb{Q}(\sqrt[4]{2}) \otimes_{\mathbb{Q}(\sqrt{2})} \mathbb{Q}(i\cdot\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i) \neq L \otimes_{L'} L = L \times L = \mathbb{Q}(\sqrt[4]{2}) \times \mathbb{Q}(\sqrt[4]{2})$.

Solución de los problemas del capítulo cuarto

Problema 1.

Problema 2.

Problema 3.

Problema 4.

Problema 5.

Problema 6.

Problema 7.

Problema 8.

Problema 9.

Problema 10.

Problema 11.

Índice alfabético

Bibliografía

1. E. Artin, Teoría de Galois, Colección de Matemáticas Nuevo Límite, Vicens-Vives, España, 1970, traducción y prólogo de R. Rodríguez Vidal.
2. M.F. Atiyah and I.G. MacDonald, Introduction to commutative algebra, Reading Mass., Addison-Wesley Publishing Company, Massachusetts, 1969.
3. N. Bourbaki, Algèbre, chapitres 4 a 7, Elements de Mathematique, Masson, Paris, 1981.
4. J. Dorronsoro and E. Hernández, Números, grupos y anillos, Addison-Wesley/Universidad Autónoma de Madrid, Madrid, 1996.
5. R. Hartshorne, Geometry: Euclid and beyond, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2000.
6. A.I. Kostrikin, Introducción al algebra, McGraw-Hill/Interamericana de España, Madrid, 1992.
7. S. Lang, Álgebra, Aguilar S.A. de ediciones, Madrid, 1971.
8. J.S. Milne, Field and Galois theory, 2002, Apuntes de clase disponible en: http://www.jmilne.org/math/CourseNotes/math594f.html.
9. J.A. Navarro González, Teoría de Galois, Sección de Matemáticas, vol. 5, Universidad de Extremadura, 1984.
10. J.A. Navarro González, Álgebra conmutativa básica, Manuales de Unex, vol. 19, Universidad de Extremadura, 1996.
11. J. Swallow, Exploratory Galois theory, Cambridge Univ. Press, New York, 2004.